Document Number

DOCUMENT ISSUER
Address

User Guide for Developing and Evaluating Security Plans for Unclassified Federal Automated Information Systems

DRAFT VERSION #6.03
FOR FINAL REVIEW

July 18, 1997

Back of cover page

(Blank)

ACKNOWLEDGMENTS

The Federal Computer Security Program Manager's Forum, an organization sponsored by the National Institute of Standards and Technology, established a workgroup to develop a guideline for developing security plans for all Federal unclassified automated information major applications and general support systems This document is the result of that effort.

The Federal Computer Security Program Managers' Forum and the National Institute of Standards and Technology gratefully acknowledges the follow people for their participation on the workgroup to develop this guideline.

Robert L. Gignilliant (Chairperson)
Department of Health & Human Services

Sadie I. Pitcher (Principal Author)
Department of Commerce, Retired

Daniel Bartko
Department of State

Judy Bloom
Department of Justice

Pauline Bowen
Food and Drug Administration

Marlene Broadus
Department of State

Doris Carter
Department of Labor

Grace Culver
Patent and Trademark Office

Brenda Dyer
Department of Justice

William Gill
Environmental Protection Agency

Alice Gannon
Office of Federal Housing

Barbara Guttman
National Institute of Standards and Technology

W. Ron Hess
National Institutes of Health

Mary Stone Holland
Department of State

Sherman Howell
Federal Deposit Insurance Corporation

Phyllis Jones
Internal Revenue Service

John Kurpiel
General Services Administration

Sonja D. Martin
Agency for International Development

Francis D. McCusker
Patent and Trademark Office

Don McGinnis
Environmental Protection Agency

Louis M. Numkin
Nuclear Regulatory Commission

Steve Posniak
Equal Employment Opportunity Commission

ACKNOWLEDGMENTS (continued)

Lloyd Reese
Department of Veterans Affairs

Phil Sibert
Department of Energy

Carl Spellacy
Office of Thrift Supervision

John Tressler
Department of Education

Rebecca Vasvary
National Oceanographic and Atmospherics Administration

Timothy M. Wooten
Farm Credit Administration

Bob Sargis
Administration for Children and Families

Steve Skolochenko
Department of Justice

Josephine M. Thomas
Small Business Administration

Timothy Turner
Office of Federal Housing

Ted I. Wells
Patent and Trademark Office

TABLE OF CONTENTS

TABLE OF CONTENTS (Continued)

INTRODUCTION

This document is intended as a guideline Federal agencies can follow in developing security plans for Federal automated information systems. Federal system security plans must meet requirements of Office of Management and Budget (OMB) Circular A-130, “Management of Federal Information Resources,” Appendix III, “Security of Federal Automated Information Resources” updated in 1996, and the “Computer Security Act of 1987," Public Law 100-235. This document incorporates all requirements originally issued as part of OMB Bulletin 90-08, “Guidance for Preparation of Security Plans for Federal Computer Systems That Contain Sensitive Information” and includes new control requirements from the updated OMB Circular A-130. This document supersedes OMB Bulletin 90-08 issued in 1990, as specified by OMB Circular A-130, Appendix III.

The objective of Federal automated information systems security planning is to improve protection of information processing resources. Plans for the protection of the resources should ensure that information and processing capabilities are reasonably protected from loss, misuse, unauthorized access or modification, unavailability, or undetected activities. Reasonable protection means that the cost of control measures does not exceed the benefits obtained by those measures (the cost of control measures is considered against the protection those measures provide, the likelihood that an adverse event will occur, and the expected loss should such an event occur).

OMB Circular A-130, Appendix III does not distinguish between sensitive and non-sensitive systems. Rather, consistent with the Computer Security Act of 1987, the Circular recognizes that Federal automated information systems have varied sensitivity and criticality. All Federal systems have some level of sensitivity and require protection as part of good management practice. All systems and applications must be covered by system security plans.

Systems/applications will be covered by an individual security plan if they are categorized as a “major application” or a “general support system.” Adequate security for other applications should be substantially provided by security of the general support systems in which they operate. For example, a department-wide Financial Management System would be a major application requiring its own security plan. A local program designed to track expenditures against an office budget might not be considered a major application and thus would be covered by a general support system security plan for an office automation system or a Local Area Network (LAN). Standard commercial-off-the-shelf software such as word processing software, electronic mail software, utility software, or other general purpose software would not typically be considered a major application and would be covered by the plans for the general support system on which they are installed. The generic term “system” is used in this document to mean either a major application or a general support system.

A security plan is required for all major applications and general support systems as part of the organization's information resources planning process. The purposes of the system security plan are to:

- Provide a basic overview of the security requirements of the subject system, and
- Describe how the requirements will be met.

The System Owner[1] is responsible for ensuring that the security plan is prepared in accordance with this guideline and for implementing the plan and monitoring its effectiveness. Security plans should reflect input from various individuals with responsibilities concerning the system, including functional "end users," Information Owners[2], the System Administrator and the System Security Manager.

All security plans should be prepared in the format outlined in this guide. The level of detail included within the plan should be consistent with the criticality and value of the system to the organization's mission (i.e., a more detailed plan is required for systems critical to the organization's mission). The security plan should fully identify and describe the controls currently in place or planned for the system.

Independent advice and comment on the security plan should be solicited prior to the plan's implementation. Independent advice and comment may be obtained from individuals within or outside the organization, who are not responsible for system development, implementation, or operation. Organizational policy should define who will provide the independent advice and comment and assign responsibility for ensuring that individual security plans have been prepared in the format outlined in this guide, that the plans contain adequate detail, and meet organizational security policy and standards. Individuals providing advice and comment should be independent of the system owner's reporting chain and have knowledge or experience in information technology (IT) security. Appropriate individuals might include an organization's IT Security Program Manager, outside contractors, or personnel from another Federal organization.

Agencies may require contractor compliance with this guide as a contract requirement. A security plan in the format specified in this document is required in those cases where vendors are operating a system under contract to the Federal Government. In those instances where a contractor or other entity (e.g., state or local government) operates a system that supports a Federal function, a security plan is required but may use an alternate format.

[1] The System Owner is responsible for defining the system's operating parameters, authorized functions, and security requirements. The information owner for information stored within, processed by, or transmitted by a system may or may not be the same as the System Owner. Also, a single system may utilize information from multiple Information Owners.

[2] The Information Owner is the manager responsible for establishing the rules for appropriate use and protection of the subject data/information. The Information Owner retains that responsibility even when the data/information are shared with other organizations.

Each security plan for a Federal system shall have four basic sections:

I. System Identification
II. Sensitivity of Information
III. System Security Measures
IV. Additional Comments

The organization of this document is described below under the section called "General Plan Content." This guide will enable an individual unfamiliar with Federal, OMB, and agency laws, regulations, policies, guidelines, and procedures to prepare a system security plan that complies with the appropriate laws, regulations, policies, guidelines, and procedures. This guideline presents the formats that should be used to develop a security plan for either a "general support system" or a "major application" as defined in OMB Circular A-130, Appendix III. The body of this guideline is divided into three major parts as follows:

GENERAL PLAN CONTENT - The first section of any security plan provides basic information concerning the system. This section applies to both "major applications" and "general support systems." Complete the information requested in this section for your system. Then go to the appropriate format for your system, (major application or general support system) and complete the required information for that system type.

FORMAT 1 — FOR MAJOR APPLICATIONS - If the system is identified as a "major application " in Section I.C. System Category, use this format.

FORMAT 2 — FOR GENERAL SUPPORT SYSTEMS - If the system is identified as a "general support system" in Section I.C. System Category, use this Format.

The appendices contain reference material and examples of security plan outlines for major applications and general support systems.

Appendix A contains a GLOSSARY of terms used in this guideline, including terms originating in OMB Circular A-130, Appendix III, and the Computer Security Act of 1987.

Appendix B contains a list of REFERENCES, including Laws and Regulations that contain provisions that must be considered for inclusion in all Federal Automated Information Systems Security programs and a list of all Federal Information Processing Standards and selected Special Publications issued by the National Institute of Standards and Technology (NIST) that contain guidance and information about automated information security subjects contained in this guideline.

Appendix C contains an outline of subsections of the security plan which must be included for a "major application."

Appendix D contains an outline of subsections of the security plan which must be included for a "general support system."

This page intentionally blank.

GENERAL PLAN CONTENT

Once completed, a security plan will contain detailed technical information about the system, its security requirements, and the controls implemented to provide protection against its risks and vulnerabilities. All security plans, at a minimum, should be marked, handled, and controlled as sensitive documents. In addition, all security plans should be dated for ease of tracking modifications and approvals. Dating each page of a security plan may be appropriate if updates are to be effected through change pages.

I. SYSTEM IDENTIFICATION

This section of the plan provides basic identifying information about the system. When completing this section, consideration should be given to potential users of the plan, e.g., senior managers responsible for approving system operations, internal and external auditors, owners of interfacing systems, and owners of supporting systems. This section must contain the following information.

I.A. Responsible Organization

This part specifies the Federal organizational sub-component responsible for the system being reported. If a State or local government or contractor performs the function, identify both the Federal and other organization and describe the relationship. Be specific about the organization and do not abbreviate. Include physical locations and addresses.

Example of Responsible Organizations

Department of Federal Government
Office of the Secretary
Information Resources Management
14th Street and Constitution Avenue, Room 1000
Washington, DC 20000

This system is maintained by:

Contractor Firm
163 Main Street, Suite 202
Washington, DC 20000

I.B. System Name/Title

Each system/application must be assigned a unique name/identifier. Assigning a unique identifier to each system helps to ensure that appropriate security requirements, based on the unique requirements for the system, are met and that allocated resources are appropriately applied. Further, the use of unique system identifiers is integral to the IT system investment models and analyses established under the requirements of the Information Technology Management Reform Act of 1996 (also known as the Clinger-Cohen Act). The identifier may be a combination of alphabetic and numeric characters and can be used in combination with the system/application name. The combination of name and unique identifier should remain the same throughout the life of the system to allow the organization to track completion of security requirements over time. In this section list the unique name/identifier for the subject system. If the system is, or has been, known by other names or acronyms, list them also.

The construction of the system identifier may be used to identify the responsible organization (System Owner) as shown in the following example.

Example System Identifier Approach

1. Each system is identified through the use of a 9-character identifier.
2. Positions 1-3 identify the primary organization, such as department or agency (e.g., DOT for the Department of Transportation or SEC for the Securities and Exchange Commission).
3. Positions 4-5 contain a code identifying the next organizational level (such as CG for Coast Guard within the Department of Transportation).
4. Positions 6-9 contain a code to identify the specific system within the organization, such as 0001 to identify the payroll system and 0237 to identify a specific office automation application.

   This allows each system to be assigned an identifier that indicates the responsible organization as well as the system.

<u>System Boundaries</u>

The boundaries of a system must be properly identified to allow for completion of the system accreditation (approval to operate) as required by OMB Circular A-130.

Defining what constitutes a “system” for the purposes of this guideline requires an analysis of system boundaries and organizational responsibilities. A system, as defined by this guideline, is identified by constructing logical boundaries around a set of processing, communications, storage, and related resources. The elements within these boundaries constitute a single system requiring a security plan. Each element of the system must—

(1) Be under the **same** direct management control,
(2) Have the **same** function or mission objective,
(3) Have essentially the **same** operating characteristics and security needs, and
(4) Reside in the **same** general operating environment.

All components of a system need not be physically connected (e.g., [1] a group of stand-alone personal computers (PCs) in an office; [2] a group of PCs placed in employees' homes under defined telecommuting program rules; [3] a group of portable PCs provided to employees who require mobile computing capability for their jobs; [4] a system with multiple identical configurations that are installed in locations with the same environmental and physical safeguards.

<u>Multiple Similar Systems</u>

An organization may have systems that differ only in the responsible organization or the physical environment in which they are located (e.g., air traffic control systems). In such instances, it is appropriate and recommended to use plans that are identical except for those areas of difference. This approach helps provide consistent levels of protection for similar systems.

Example for Multiple Similar Systems

A general support system in Washington, D.C. provides distributed application and telecommunications support for three remote sites located in California, Colorado, and Alaska. A separate security plan may be prepared for each location (a total of four plans) or a single plan may be prepared with abbreviated, subordinate plans for each remote site. Specifically, a "master plan" would be developed for the Washington, D.C. site by the organization that has responsibility for system development, operation, and maintenance. Remote site security plans would be a shorter "system site plan" that references the security plan for the Washington, D.C. system (using its unique identifier) and contains information unique to the site (e.g., physical, environmental, responsible individuals, hardware, contingency plan, risk assessment, certification and accreditation/approvals and milestone or completion dates for planned controls). System plans that reference the master plan must also be listed in the master plan by their unique identifiers.

This approach facilitates analysis of the security provided to the entire distributed system and helps ensure that there are no weak security links.

I.C. System Category

Categorize each system as either a “**major application**” or as a “**general support system.**” All applications must be covered by a security plan. They will either be covered individually if they have been designated as a major application, or within the security plan of the appropriate general support system. A particular system may be designated as a major application even though it is also supported by a system that has been designated as a general support system. For example, a LAN may be designated a general support system and have a security plan. The organization’s accounting system may be designated as a major application even though it is supported by the computing and communication resources of the LAN.

Major Application

All Federal applications have value and require some level of protection. Certain applications, because of the information they contain, process, or transmit or because of their criticality to the organization’s missions, require special management oversight. These applications are major applications.

Agencies are expected to exercise management judgement in determining which of their applications are major and to ensure that the security requirements of non-major applications are discussed as part of the security plan for the appropriate general support systems.

Major applications are systems that perform clearly defined functions for which there are readily identifiable security considerations and needs (e.g., an electronic funds transfer system). A major application might comprise many individual programs and hardware, software, and telecommunications components. These components can be a single software application or a combination of hardware/software focused on supporting a specific mission-related function. A major application may also consist of multiple individual applications if all are related to a single mission function (e.g., payroll or personnel).

If you define your system category as major application, and you are a user of another organization's general support system, it is your responsibility to—

- Notify the system owner that your application is critical or contains sensitive information and provide specific security requirements;

- Provide a copy of your major application’s security plan to the operator of the general support system;

- Request a copy of the system security plan for the general support system and ensure it provides adequate protection for your application and information; and

- Include a reference to the general support system security plan, including the unique name/identifier information, in item I.F. System Environment and Special Considerations, of your plan.

General Support System

A general support system is an interconnected set of information resources under the same direct management control that share common functionality. A general support system normally includes hardware, software, information, data, applications, communications, facilities, and people and provides support for a variety of users and/or applications. A general support system, for example, can be a —

- LAN including smart terminals that support a branch office,
- Backbone (e.g., agency-wide),
- Communications network,
- Departmental data processing center including its operating system and utilities,
- Tactical radio network, or
- Shared information processing service organization.

Although the Computer Security Act of 1987 required the development of security plans only for computer systems that contained sensitive information, OMB Circular A-130, Appendix III, issued in 1996, broadened that to include **all** Federal interest general support systems. Specifically, it states, “Given the expansion of distributed processing since passage of the Act, the presumption in the Appendix is that all general support systems contain some sensitive information which requires protection to assure its integrity, availability, or confidentiality and therefore all systems require security plans.”

Include information about all applications running on this system in section I.E. General Description/Purpose. Be sure to discuss specific requirements separately for each application.

I.D. System Operational Status

Indicate one of the following for the system’s operational status.

- *Operational* — the system is operating.

- *Under development* — the system is being designed, developed, or implemented.

- *Undergoing a major modification* — the system is undergoing a major conversion or transition.

If the system is under development or undergoing a major modification, provide information about the methods used to assure that up-front security requirements are included. Include specific controls in the appropriate sections in Part III of the plan.

I.E. General Description/Purpose

Present a brief (1-3 paragraphs) description of the function and purpose of the system (e.g., economic indicator, network support for an organization, business census data analysis, crop reporting support).

Automated information system security requirements should be coordinated between end users and those responsible for any support system(s) being used. Plans for such requirements must be based on an understanding of what is to be protected and the type and degree of protection required. Thus, if this is a general support system, the nature of the uses of the applications supported should also be described.

List all applications supported by the general support system. Specify if the application is or is not a major application, and include unique system identifiers, where applicable. Discuss each application's function and the type of data/information processed. Include a list of user organizations and a general description of the type of information and processing provided. Request information from the application owners (and a copy of the security plans for major applications) to ensure their requirements are met.

Include a list of user organizations and whether they are internal or external to the system owner's organization.

I.F. System Environment and Special Considerations

Provide a brief (1-3 paragraphs) general description of the technical system. Include any environmental factors that raise special security concerns, such as:

- The system is connected to the Internet;
- It is located in a harsh or overseas environment;
- Software is rapidly implemented;
- The software resides on an open network used by the general public or with overseas access;
- The application is processed at a facility outside of the agency's control; or
- The general support mainframe has dial-up lines.

Describe the primary computing platform(s) used (e.g., mainframe, mini-computer, micro-computer(s), LAN or Wide Area Network (WAN). Include a general description the principal system components, including hardware, software, and communications resources. Discuss the type of communications included (e.g., dedicated circuits, dial circuits, public data/voice networks). Describe controls used to protect communication lines in the appropriate sections of the security plan.

Note: Include any security software protecting the system and information. Describe in general terms the type of security protection provided (e.g., access control to the computing platform and stored files at the operating system level or access to data records within an application). Include only controls that have been implemented or are planned, rather than listing the controls that are available in the software. Controls that are available, but not implemented, provide no protection.

Example System Environment and Special Considerations

The system is physically housed in a Government-owned building located in Washington, D.C. The entire building is occupied by Department of ABC Civil Service and contractor personnel and is not open to the general public. The system uses mainframe hardware. The system consists of a Brand X 9999 supercomputer and a Brand Y 8888 mainframe configuration. The operating system running on the Brand X 9999 system is OS-YYYY and on the Brand Y 8888 system is OS-OOOO1. The security software protecting all system resources from the top levels are XYZ and PDQ. DOA-XX-0123, a complex wide area communication network system, provides support to client agencies nationwide.

I.G. System Interconnection/Information Sharing

System interconnection is the direct connection of systems for the purpose of sharing information resources. Information sharing is the exchange of information between systems. Information sharing may/may not be achieved through a system interconnection.

System interconnection, if not appropriately protected, may result in a compromise of all connected systems and the data they store, process, or transmit. Written management authorization (often in the form of a Memorandum of Understanding or Agreement), should be obtained prior to connecting with other systems and/or sharing sensitive data/information. The written authorization should detail the rules/controls that must be maintained by the interconnecting systems and for protecting the shared information. A description of the rules for interconnecting systems and for protecting shared data must be included in the security plan in Section III.D. “Rules.”

It is important that system operators, information owners, and management obtain as much information as possible about the vulnerabilities associated with system interconnection and information sharing and the increased controls required to mitigate those risks.   The security plan for the systems often serves as a mechanism to effect this security information exchange and allow management to make informed decisions regarding risk reduction and acceptance.

System connectivity varies. For example, some systems will choose to isolate themselves (no connectivity), others will restrict access such as allowing only electronic mail (E-mail) connections or remote access only with sophisticated authentication devices. Others will be fully open, allowing unrestricted access between systems. The management decision to interconnect should be based on the availability and use of technical and non-technical safeguards and be consistent with the acceptable level of risk defined in the system rules.

The security plan with the associated written authorization, provides information owners with assurance that information shared is appropriately protected, equivalent to the protection provided by the information owner. This protection requirement typically focuses on protection against unauthorized disclosure and alteration with little emphasis on availability. This focus corresponds with the concern of the information owner. Availability concerns are typically the focus of concern for the users of the shared information.

Include in this section the following information concerning the authorization for the connection to other systems or the sharing of information:

- List of authorized systems (including Internet),
- Unique system identifiers, if appropriate,
- Name of system(s),
- Organization owning the other system(s),
- Type of interconnection (TCP/IP, Dial, SNA, etc.),
- Short discussion of major concerns or considerations in determining interconnection (do not repeat the system rules included in Section III.D.),
- Name and title of authorizing management official(s),
- Date of authorization,
- System of Record, if applicable (Privacy Act data),
- Sensitivity level of each system,
- How the systems will interact, and
- Security concerns and Rules of Behavior of the other systems that need to be considered in the protection of this system (highlight unique security concerns and Rules of Behavior for interconnected systems in Section III).

I.H. Information Contact(s)

List the name, title, organization, and telephone number of one or more persons designated to be the point(s) of contact for this system. One of the contacts given should be identified as the system owner. The designated persons should have sufficient knowledge of the system to be able to provide additional information or points of contact, as needed.

Example Information Contacts

Ms. Jane Smith (System Owner)
ABC Division Chief
1111 West Street, Room 222
Rockville, MD 20852
(301) 123-4567

Mr. John Doe
Program Manager
ABC Division
1111 West Street, Room 233
Rockville, MD 20852
(301) 123-8910

II. SENSITIVITY OF INFORMATION HANDLED

This section provides a description of the types of information handled by the system and/or the criticality of the information to accomplishing the organization's mission. The sensitivity and criticality of the information stored within, processed by, or transmitted by a system provides a basis for the system's security requirements. The description will provide information to a variety of users, including:

- Analysts/programmers who will use it to help design appropriate security controls;
- Internal and external auditors evaluating system security measures; and
- Managers making decisions about the reasonableness of security countermeasures.

The nature of the information sensitivity and criticality must be described in this section. The description must contain information on applicable laws and regulations affecting the system and a general description of sensitivity as discussed below.

II.A. Applicable Laws or Regulations Affecting the System

List any laws or regulations that establish specific requirements for **confidentiality**, **integrity**, or **availability** of data/information in the system. Examples might include the Privacy Act or a specific statute or regulation concerning the information processed (e.g., tax or census information). This should **not** be a list of technical standards concerning how to protect systems once the need for such protection has been determined. For this reason, the Computer Security Act of 1987 should not be listed here.

If the system processes records subject to the Privacy Act, include the number and title of the Privacy Act system(s) of records and whether the system(s) are used for computer matching activities.

List all laws and regulations that apply to the system's particular information protection requirements. The sample list below contains a few of the general laws and regulations that may apply. Add any organizational regulations that apply and any Federal regulations or laws that apply to the specific information or mission. List any guidance or regulations that designate any specific handling requirements. At a minimum, OMB Circular A-130 and agency Automated Information Systems (AIS) security policies apply.

Example Applicable Laws or Regulations Affecting the System

Privacy Act of 1974 (PL-93-579)
Paperwork Reduction Act of 1980 as amended in 1995
OMB Circular A-130
OMB Circular A-123
Departmental Automated Information Systems Security Policies

(See Appendix B of this guide for additional information.)

II.B. General Description of Sensitivity

Both information and information systems have distinct life cycles. It is important that the degree of sensitivity of information be assessed by considering the requirements for **availability, integrity, and confidentiality** of the information. This process should occur at the beginning of the information system's life cycle and be re-examined during each life cycle stage. In addition, the rules of behavior for dealing with the information should be established initially and refined as necessary during each life cycle stage.

The concept that is of paramount importance is the integration of security considerations early in the life cycle to avoid costly retrofitting of safeguards. Establishing the needs for information protection is best accomplished during the information life cycle model (creation or collection, processing, dissemination, use, storage, and disposition life cycle stages). The information system life cycle is typically characterized by the initiation, development, operation, and termination stages. If security has not been assessed previously for the information that will be stored and processed in an automated system, then this process should be included in the initiation stage of the system's life cycle.

Security requirements established for the information life cycle stages can be easily incorporated into the information system life cycle as system requirements established during the initiation phase. In addition, security requirements of systems that interact with the information system under development should be evaluated for relevance and inclusion into the system requirements and rules of behavior. The security considerations and rules of behavior will become more detailed and may need to be refined throughout the life cycle.

Technical considerations may alter some initial approaches to information protection as the system progresses through its life cycle stages. The information system development and management roles and associated required resources (e.g., Government vs. contract) should be assessed in the initiation stage and periodically reevaluated to ensure that adequate safeguards, alternatives, and rules are in place and implemented as needed during the information system's life cycle.

The purpose of this section is to indicate the type of protection needed for the system. A system may need protection for one or more of the following reasons:

- *Confidentiality*

  The system contains information that requires protection from unauthorized disclosure.

Example of Information Requiring Protection — Confidentiality

Timed dissemination information (e.g., crop report information), personal information (covered by Privacy Act), proprietary business information (e.g., business plans), or defense classified information.

- *Integrity*

  The system contains information which must be protected from unauthorized, unanticipated, or unintentional modification.

Example of Information Requiring Protection — Integrity

Census information, economic indicators, or financial transaction systems.

- *Availability*

  The system contains information or provides services which must be available on a timely basis to meet mission requirements or to avoid substantial losses.

Example of Information Requiring Protection — Availability

Systems critical to safety, life support, hurricane forecasting, or budgets.

Describe, in general terms, the information handled by the system and the need for protective measures.

- Relate the information handled to each of the three basic protection requirements above (**confidentiality**, **integrity**, and **availability**).

- Include a statement of the estimated risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information in the system. To the extent possible, describe this impact in terms of cost, inability to carry out mandated functions, timeliness, etc.

For each of the three categories (**confidentiality**, **integrity**, and **availability**), indicate if the protection requirement is:

- *High* — a critical concern of the system;

- *Medium*— an important concern, but not necessarily paramount in the organization's priorities; or

- *Low* — some minimal level or security is required, but not to the same degree as the previous two categories.

Examples of a General Protection Requirement Statement

A high degree of security for the system is considered mandatory to protect against unauthorized disclosure, modification, and denial of service. The protection requirements for all applications are critical concerns for the system.

or

Confidentiality is not a concern for this system as it contains information intended for immediate release to the general public concerning severe storms. The integrity of the information, however, is extremely important to ensure that the most accurate information is provided to the public to allow them to make decisions about the safety of their families and property. The most critical concern is to ensure that the system is available at all times to acquire, process, and provide warning information immediately about life threatening storms.

Example Confidentiality Considerations	
Evaluation	**Comment**
High *or*	The application contains proprietary business information and other financial information, which, if disclosed to unauthorized sources could cause unfair advantage for vendors, contractors or individuals and could result in financial loss or adverse legal action to user organizations.
Medium *or*	Security requirements for assuring confidentiality are of moderate importance. Having access to only small portions of the information has little practical purpose and the satellite imagery data does not reveal information involving national security.
Low	The mission of this system is to produce local weather forecast information which is made available to the news media forecasters and the general public at all times. None of the information requires protection against disclosure.

Example Integrity Considerations	
Evaluation	**Comment**
High *or*	The application is a financial transaction system. Unauthorized or unintentional modification of this information could result in fraud, under or over payments of obligations, fines or penalties resulting from late or inadequate payments, and loss of public confidence.
Medium *or*	Assurance of the integrity of the information is required to the extent that destruction of the information would require significant expenditures of time and effort to replace. Although corrupted information would present an inconvenience to the staff, most information, and all vital information, is backed up by either paper documentation or on disk.
Low	The system mainly contains messages and reports. If these messages and reports were modified, by unauthorized, unanticipated or unintentional means, employees would detect the modifications; however, these modifications would not be a major concern for the organization.

Example Availability Considerations	
Evaluation	**Comment**
High *or*	The application contains personnel and payroll information concerning employees of the various user groups. Unavailability of the system could result in inability to meet payroll obligations and could cause work stoppage and failure of user organizations to meet critical mission requirements. The system requires 24-hour access.
Medium *or*	Information availability is of moderate concern to the mission. Macintosh and IBM PC availability would be required within the 4 to 5 day range. Information backups maintained at off-site storage would be sufficient to carry on with limited office tasks.
Low	The system serves primarily as a server for E-mail for the seven users of the system. Conference messages are duplicated between Seattle and D.C. servers. Should the system become unavailable, the D.C. users would connect to the Seattle server and continue to work with only the loss of old mail messages.

III. SYSTEM SECURITY MEASURES

This section describes the control measures (**in place** or **planned**) that are intended to meet the protection requirements of the major application or general support system. The types of control measures shall be consistent with the need for protection of the major application or general support system described in the previous section. Include any security concerns or Rules of Behavior identified in Section I.G., “System Interconnection/Information Sharing.” The following information should be included in this section of the security plan.

III.A. Risk Assessment and Management

OMB Circular A-130, Appendix III, re-issued in 1996, no longer requires the preparation of a formal risk analysis. It does, however, require an assessment of risk as part of a risk-based approach to determining adequate, cost-effective security for a system. Risk assessment and risk management are crucial elements of the security planning process which includes—

- Identification of information and other system assets,

- Valuation of the system and associated assets,

- Identification of threats that could affect system confidentiality/integrity/availability,

- Identification of system vulnerabilities through which the identified threats could adversely affect the system or its associated assets,

- Estimation of potential impacts from the occurrence of a threat,

- Identification of security measures that can correct identified vulnerabilities or mitigate the system impact of a threat that does occur, and

- Selection of security measures for implementation based on their cost and benefits (i.e., ability to reduce the level of system/asset loss, compromise, or disruption of operations). Additional guidance on effective risk assessment is available in "An Introduction to Computer Security: The NIST Handbook" (March 16, 1995).

Risk analyses are excellent tools for identifying vulnerabilities and providing the cost/benefit information necessary to support the risk management process. System Owners may elect to use a formal quantitative or qualitative risk analysis to support their decisions regarding the most appropriate security measures for their system and operating environment. Regardless of which risk analysis methodology is selected for use, the cost of performing the risk analysis should not be excessive in comparison with its benefits. Maintaining a risk analysis with periodic updates is often a cost-effective approach to assess current risks.

Describe the Risk Assessment Approach

In this section, describe the methods used to assess the nature and level of risk to the system. Be specific in describing whether the methodology addresses the crucial elements of the security planning process listed above. For example, did the selected risk assessment methodology identify threats, vulnerabilities, and the additional security measures required to mitigate or eliminate the potential that those threats/vulnerabilities could have on the system or its assets?

Include the date that the system risk assessment was conducted. State how the identified risks relate to the requirements for confidentiality, integrity, and availability determined for the system.

If there is no risk assessment for your system, include a milestone date (month and year) for completion of the risk assessment. If the risk assessment is more than three years old or there have been major changes to the system or its functions, include a milestone date (month and year) for completion of a new or updated risk assessment. Assessing the risk to a system should be an on-going activity to ensure that new threats and vulnerabilities are identified and appropriate security measures are implemented.

<u>Other System Evaluation Approaches</u>

Other types of security reviews, assessments, or evaluations may be conducted on your system by internal or external organizations or groups. These reviews may provide information useful in assessing the system’s risk. Such reviews include ones conducted on your facility or site by physical security specialists from other components of your organization; system audits; or security program reviews performed by your Inspector General's staff, personnel from the National Security Agency, NIST, or a contractor. These reviews may evaluate the security of the total system or a logical segment/subsystem. The system descriptions, findings, and recommendations from these types of reviews may provide information to support your risk assessment and risk management process. If other types of security evaluations have been conducted on your system, include information about who performed the review, when the review was performed, the purpose of the review, the findings, and the actions taken as a result of the review.

Example of Other Reviews/Evaluations

The National Security Agency performed an INFOSEC Enhancement Review of the computer center in January 1996, and recommended countermeasures for improving protection of dial-in communication lines. Based on these recommendations, dial-back was implemented in April 1996.

III.B. Review of Security Controls

OMB states that at least every three years, an independent management review or audit of the security controls for the system must be performed. This review or audit should be independent of the manager responsible for the major application or general support system. Independent audits can be internal or external but should be performed by an individual or organization free from personal and external factors which could impair their independence or their perceived independence (e.g., they designed the system under review). For some high risk systems with rapidly changing technology, three years may be too long and reviews may need to be conducted more frequently. These independent management reviews/audits are in addition to system testing and the types of reviews listed in Section III.A. The objective of these reviews is to provide verification that the controls selected and/or installed are adequate to provide a level of protection to reach an acceptable level of risk for the system. The determination that the level of risk is acceptable must be made relative to the system requirements for confidentiality, integrity, and availability as well as the identified threats.

The security of a system may degrade over time, as the technology changes, the system evolves, or people and procedures change. Periodic reviews provide assurance that management, operations, personnel, and technical controls are functioning effectively and providing adequate levels of protection.

The type and rigor of review or audit should be commensurate with the acceptable level of risk that is established in the rules for the system and the likelihood of learning useful information to improve security. Technical tools such as virus scanners, vulnerability assessment products (which look for known security problems, configuration errors, and the installation of the latest hardware/software “patches”), and penetration testing can assist in the on-going review of system security measures. These tools, however, are no substitute for a formal management review at least every three years.

Depending upon the risk and magnitude of harm that could result, weaknesses identified during the review of security controls should be reported as deficiencies in accordance with OMB Circular No. A-123, “Management Accountability and Control” and the Federal Managers' Financial Integrity Act. The lack of a basic management control such as assignment of security responsibility, a workable security plan, or management approval to operate should be reported as a material weakness.

Describe the Type of Independent Security Review and Its Findings

Include information about the last independent audit or review of the system and who conducted the review. Discuss any findings or recommendations from the review and include information concerning correction of any deficiencies or completion of any recommendations. Indicate if the review identified a deficiency reportable under OMB Circular No. A-123 or the Federal Managers' Financial Integrity Act. Indicate in this section if an independent audit or review has not been conducted on this system.

III.C. Applicable Guidance

Indicate, to the extent practical, specific standards or other guidance used in the design, implementation, or operation of the protective measures used on the system (e.g., relevant Federal or industry standards). List any Federal Information Processing Standards (FIPS) issued by NIST that may apply. Include agency guidance documents.

Example of Applicable Guidance

Various FIPS Publications (if possible, list by number)
Life Cycle Management Regulation (list by organization number)
OMB Circulars A-130, A-123, and A-127
Departmental Policies (title and number)
Agency Directives (title and number)
Organization Specific Policies or Procedures (title and number)

III.D. Rules

Include the “rules of behavior” that have been established for the system.

Note: If the set of rules are contained in a separate document, attach that document as an appendix to the plan and reference the appendix number in this section.

A set of rules of behavior must be established for each system. The acceptable level of risk for the system must be established and should form the basis for determining the rules, which shall be based on the needs of the users of the system. The security required by the rules is only as stringent as necessary to provide adequate security for the system and the information it contains.

The rules of behavior shall clearly delineate responsibilities and expected behavior of all individuals with access to the system. They shall also include appropriate limits on interconnections to other systems and define service provision and restoration priorities. The rules must be clear about the consequences of behavior not consistent with the rules. Rules should be in writing and will form a basis for computer security awareness activities and training. (Guidance that can be used by system owners in establishing the system-specific rules will be available from NIST or the Federal Computer Security Program Manager’s Forum).

The rules of behavior should cover such matters as work at home, dial-in access, connection to the Internet, use of copyrighted works, unofficial use of Government equipment, the assignment and limitation of system privileges, and individual accountability. Rules should reflect administrative and technical security controls in the system. For example, rules regarding password use should be consistent with technical password features in the system. Such rules would also include limitations on changing information, searching databases, or divulging information. Rules of behavior may be enforced through administrative sanctions specifically related to the system (e.g., loss of system privileges) or through more general sanctions as are imposed for violating other rules of conduct. In addition, the rules should specifically address restoration of service as a concern of all users of the system.

The rules of behavior should be made available to every user prior to receiving authorization for access to the system.

III.E. Security Control Measures

This is the most important part of the security plan. It contains a description of the security measures that protect system confidentiality, integrity, and availability. Proper documentation of this section aids management in determining if the level of security provided is adequate and in identifying what additional actions and/or resources (if any) are required for the system to meet operational and security requirements. In addition, this section establishes the milestones for completing requirements. This section can be used as an internal management planning, monitoring, and decision-making tool.

Control measures included should be addressed from the perspective of the individual having direct management control of the system. For each system, only the set corresponding to the system category designated under Section I.C. *System Category* needs to be completed. Two sets of controls are provided and discussed on subsequent pages. **Format 1** is for **major applications**; **Format 2** is to be used for **general support systems**.

The controls described below are derived from requirements and guidance in the Computer Security Act; OMB Circular No. A-130, Appendix III; and applicable Federal Information Processing Standards and Special Publications produced by NIST.

Security Control Measure Status

For each control measure on the appropriate list, specify whether controls are "**In-Place**," "**Planned**," "**In-Place and Planned**," or "**Not Applicable.**" Specifying "**In-Place**" is not adequate. A general description of what is in place or planned must be included. For each question, describe the control measures in enough detail to determine if they are adequate. If a control is planned, provide an expected milestone date (month and year) when it will be in place.

- **In-Place** controls are operational and judged to be effective. Use general terms for describing all controls that are currently in place.
- **Planned** controls are specific control measures (e.g., new, enhanced) that will be implemented for the system. Provide a general description of the planned measures, resources involved, and milestone operational dates (month and year).
- **In-Place and Planned** controls are those where some measures are operational, while others are planned. Include a general description of the measures in place and those planned, including resources involved and expected operational dates.
- **Not Applicable** describes a type of control measure that is not needed, cost-effective, or appropriate for this system. A control that may be appropriate but not cost-effective should be highlighted as management may disagree during certification and accreditation. If you identify a control as "**Not Applicable,**" your answer should justify that determination, as all of the listed controls are required by various regulations.

Note: For operational systems, some specific controls of a given type may be "**In Place,**" while others may be "**Planned**." For systems under development or undergoing a major modification, it is expected that many measures will be "**Planned**."

This page intentionally blank.

FORMAT 1 — MAJOR APPLICATIONS

Note: If the system is identified as a **major application** in Section I.C., *System Category*, use this format. If the system is identified as a **general support system**, use Format 2.

Begin each of the following control sections by indicating the appropriate "Security Control Measure Status" — ***"In-Place," "Planned," "In-Place and Planned,"*** *or* ***"Not Applicable"*** *before discussing the control information. For sections where some controls are* ***"In-Place"*** *while others are* ***"Planned"*** *list or discuss each category separately, and include milestone dates for completion of the planned actions.*

III.E.1. MANAGEMENT CONTROLS

Describe the overall management controls of the application.

III.E.1.a. Assignment of Security Responsibility

Major applications are high risk applications requiring special management attention. Major applications usually support a single agency function and are often supported by one or more general support systems. It is important, therefore, that an individual be assigned responsibility (in writing) to ensure that the application has adequate security. To be effective, this individual should be knowledgeable of the information and process supported by the application and in the management, personnel, operational, and technical controls used to protect the application.

Include the name, title, and telephone number (where applicable) of the individual who has been assigned responsibility for the security of the application and who will act as the Automated Information System Security Officer (AISSO). Indicate whether the idividual has been designated in writing as the AISSO.

Example Security Contact

Bill Smith, AISSO
Computer Specialist
ABC Division, XYZ Branch
1111 West Street, Room 444
Rockville, MD 20852
(301) 123-1213

III.E.1.b. Personnel Security

The greatest harm/disruption to a system comes from the actions of individuals, both intentional and unintentional. All too often systems experience disruption, damage, loss, or other adverse impact due to the well-intentioned actions of individuals authorized to use or maintain a system (e.g., the programmer who inserts “one minor change” then installs the program into the production environment without testing). Personnel controls (technical, operational, and management) are intended to prevent the occurrence or minimize the impact of undesirable events caused by the actions of individuals (authorized as well as not authorized for system access). Such controls include individual accountability, least privilege, and separation of duties.

Individual accountability consists of holding individuals responsible for their actions. In an application system, accountability is accomplished by identifying and authenticating individuals and providing the capability to associate them with their actions (install a new program, execute a program) relative to the system. This may be accomplished through user identifiers assigned to each individual, audit trails, and/or pattern analysis of system usage data.

Least privilege is the practice of restricting a user’s access (to data files, to processing capability, or to peripherals) and type of access (e.g., read, write, execute, delete) to the minimum necessary to perform his or her job.

Separation of duties is the practice of dividing the steps in a critical function among different individuals to ensure that no individual has all necessary authority or information access which could result in fraudulent activity. For example, in a financial application, an individual should not be allowed to establish accounts and also be authorized to make payments to those accounts. Another example might be to have one programmer create a segment of application code, a manager authorize its implementation, and a second application programmer implement the code. Such controls keep a single individual from subverting a critical process or inserting that “one last minor change” without test. Separation of duties may be enforced through administrative or technical controls.

Federal policies require that all automated data processing (ADP) positions be evaluated and a sensitivity level be assigned to the position description. A background investigation is required for all employees and contractors assigned to sensitive positions. The requirement for background screening includes both Government and contractor personnel who design, implement, maintain, or use the system. The type of background investigation required is determined by the sensitivity level assigned to the individual position description, the individual’s level of system responsibility and authority, and an assessment of the adequacy of the control environment.

Where technical and administrative controls cannot adequately protect the application or the information it contains, individuals should be screened at a level commensurate with the risk of harm they could cause. Such screening is to be performed prior to the individual's being authorized to access the application and periodically thereafter. For most major applications, management controls such as individual accountability, separation of duties, and limitations on the processing privileges of individuals, are generally more cost-effective personnel security controls than background screening.

Include detailed information about any personnel controls that are not included in other sections of this security plan, (i.e., technical controls and rules). Also include a short discussion or list of controls discussed in detail in other sections of the plan, or reference section numbers of this plan where detailed information is included. These discussions should include the following specific items:

- A statement as to whether all positions have been reviewed for sensitivity level. If all positions have not been reviewed, state the planned date for completion of position sensitivity analysis.

- A statement as to whether individuals have received the background screening appropriate for the position to which they are assigned. If all individuals have not had appropriate background screening, include the date by which such screening will be completed.

- If individuals are permitted system access prior to completion of appropriate background screening, describe the conditions under which this is allowed and any compensating controls to mitigate the associated risk.

This page intentionally blank.

III.E.2. DEVELOPMENT / IMPLEMENTATION CONTROLS

Development/implementation controls are procedures to—

- Assure that adequate protection is built into the application during development; and
- Ensure continued operation at an acceptable level of risk during the installation, implementation, and maintenance and operation stages.

III.E.2.a. Authorize Processing

Systems must have specific authorization to initiate and continue production operations. The authorization of a system to process information, granted by a senior management official, is an important quality control and is required by OMB Circular A-130. In this section of the plan, include the following information:

Certification: Date of certification, name and title of Certifying Official
If not certified, name and title of manager requesting approval to operate and date of request.

Accreditation: Date of approval to process/accreditation, name and title of individual approving/accrediting the system for processing.

If the application system has not been certified or accredited, include reasonable milestone dates (month and year) for completing all requirements and obtaining certification and accreditation for the system.

Approval to Process/Accreditation

Some agencies refer to the process of granting systems approval to operate as accreditation. By approving/accrediting operation of a system, a manager—

- Accepts the associated risks to the organizational mission and assets (hardware, software, data); and
- States that there is reasonable assurance that system assets are adequately protected against waste, fraud, and abuse and that “the system does what it is supposed to do, and nothing more.”

Approval to operate is a decision that should be made by an individual with the authority to budget for and allocate resources to resolve concerns that create unacceptable risks. The position of this individual will vary between organizations. Approval to operate is not a decision that may be made by the security staff.

Both the security official and the approving management official have security responsibilities. The security official is closer to the day-to-day operation of the system and thus will direct, perform, or monitor security tasks. The approving official will have management responsibility for or within the organization supported by the system.

Management authorization should be based on an assessment of management, operational and technical controls. Since the security plan establishes the system protection requirements and documents the appropriate controls necessary to reach an acceptable level of risk, it forms the basis for the approval to operate, supplemented by specific studies as needed. In addition, the periodic review of controls should contribute to future decisions regarding the approval to operate.

Management approval/authorization to process should be granted prior to initial implementation and at least every three years thereafter or when there are major changes to the system. System approval decisions and the associated analyses should be performed more often where there is a high risk and potential magnitude of harm.

Some agencies have established the system approval process as a formal accreditation procedure where the approving authority is termed the Designated Approving/ Accreditation Authority (DAA). Formalization of the system approval process reduces the potential that systems will be placed into a production environment without appropriate management review.

Certification Reviews

Prior to accreditation, each application system should undergo a technical evaluation to ensure that—

- It meets applicable Federal laws, regulations, policies, guidelines, and standards;
- In-place and planned security safeguards appear to be adequate and appropriate for the system; and
- In-place safeguards are operating as intended.

These technical reviews are generally termed “certification reviews” and are often independent reviews. Certification reviews are intended to provide a technical analysis of system controls and other security arrangements in support of a management decision as to whether an “authorization to process” should be granted (e.g., the system is accredited for processing). Technical certification reviews (such as those using the methodology in FIPS Publication 102 “Guidelines for Computer Security

Certification and Accreditation") provide useful information to assist management in authorizing a system, particularly when combined with a review of the broad behavioral controls envisioned in the security plan, as required by OMB Circular A-130.

In some agencies, a certification review includes a specific system test and evaluation (ST&E). The ST&E is a formal test of the system and its associated controls to ensure that in place controls are functioning.

Some agencies have established formal certification procedures that require that systems must be "certified" before they may be submitted for an approval to operate decision. In these cases, a management official with a technical background typically acts as the Certifying Official. The Certifying Official issues a certification statement and prepares and forwards an approval/accreditation package to the individual designated as the approving official or DAA requesting formal approval to process for the system.

III.E.2.b. Security Specifications

Appropriate technical, administrative, physical, and personnel security requirements should be specified for the application. Among the questions that should be addressed are the following:

- During the application design, were security requirements identified?
- Were the appropriate security controls included in the specifications for the application development?
- Have security controls been added since development (i.e., during system operation and maintenance)?
- If this is a purchased commercial application or the application contains commercial, off-the-shelf components, were security requirements identified and included in the acquisition specifications?

Include a general discussion of any specifications that were used and whether they are being maintained.

III.E.2.c. Design Review and Testing

A design review and systems test should be performed prior to placing the application into operation, to assure that it meets security specifications. In addition, if new controls are added to the application or to any support systems, additional acceptance tests of those new controls must be performed. This ensures that new controls meet security specifications and do not conflict with or invalidate existing controls. The results of the design reviews and system tests should be fully documented, updated as new reviews or tests are performed, and maintained in the official agency records.

In this section, discuss when and by whom the design reviews and systems tests were conducted. Include information about additional design reviews and systems tests for any new controls added after the initial acceptance tests were completed. Discuss whether the documentation of these reviews and tests has been keep up to date and maintained in the agency records.

III.E.3. OPERATIONAL CONTROLS

Operational controls are the day-to-day procedures and mechanisms used to protect production applications (or planned applications when they become operational). Operational controls affect the application and system environments.

III.E.3.a. Physical and Environmental Protection

Discuss the physical protection in the area where application processing takes place (e.g., locks on terminals, physical barriers around the building and processing area).

Appropriate and adequate controls will vary depending on the individual system requirements. The example list shows the types of controls in this category. The list is not intended to be all inclusive or to imply that all systems should have all controls listed.

.

Example Physical/Environmental Controls

In Place

- Card keys for building and work area entrances
- 24-hour guards at all entrances/exits
- Cipher lock on computer room door
- Raised floor in computer room
- Dedicated cooling system
- Humidifier in tape library
- Emergency lighting in computer room
- Four fire extinguishers rated for electrical fires
- One B/C rated fire extinguisher
- Smoke, water, and heat detectors
- Emergency power-off switch by exit door
- Surge suppressor
- Emergency replacement server
- Zoned dry pipe sprinkler system
- Uninterruptable power supply for LAN servers
- Power strips/suppressors for peripherals
- Power strips/suppressors for computers
- Controlled access to file server room

Planned

- Plastic sheets for water protection, August 1997
- Closed-circuit television monitors, January 1998

III.E.3.b. Production, Input/Output Controls

Discuss controls over the marking, handling, processing, storage, and disposal of input and output information and media, as well as access controls (such as labeling and distribution procedures) for the information and media. The discussion should include consideration of the following:

- Procedures to ensure unauthorized individuals cannot read, copy, alter, or steal printed or electronic information.
- Procedures for ensuring that only authorized users pick up, receive, or deliver input and output information and media.
- Audit trails for receipt of sensitive inputs/outputs.
- Procedures for restricting access to output products.
- Procedures and controls used for transporting or mailing media or printed output.
- Internal/external labeling for appropriate sensitivity (e.g., Privacy Act, Proprietary, Confidential).
- External labeling with special handling instructions (e.g., log/inventory identifiers, controlled access, special storage instructions, release or destruction dates).
- Audit trails for inventory management.
- Media storage vault or library physical and environmental protection controls and procedures.
- Procedures for sanitizing electronic media for reuse (e.g., overwrite or degaussing of electronic media).
- Procedures for controlled storage, handling, or destruction of spoiled media or media that can not be effectively sanitized for reuse.
- Procedures for shredding or other destructive measures for hardcopy media when no longer required.

III.E.3.c. Contingency Planning

Procedures are required that will permit the organization to continue essential functions if information technology support is interrupted. These procedures (contingency plans, business interruption plans, continuity of operations plans) should be coordinated with the backup, contingency, and recovery plans of any general support systems, including networks used by the application. The contingency plans should ensure that interfacing systems are identified and contingency/disaster planning coordinated.

Describe the procedures (contingency plan) that would be followed to ensure the application continues to be processed if the supporting IT systems were unavailable and provide a reference to the detailed plans. Include consideration of the following questions in this description:

- Are tested contingency plans in place to permit continuity of mission-critical functions in the event of a catastrophic event?

- Are tested disaster recovery plans in place for all supporting IT systems and networks?

- Are formal written emergency operating procedures posted or located to facilitate their use in emergency situations?

- How often are contingency, disaster, and emergency plans tested?

- Are all employees trained in their roles and responsibilities relative to the emergency, disaster, and contingency plans?

Include descriptions of the following controls.

- Any agreements for backup processing (e.g., hotsite contract with a commercial service provider).

- Documented backup procedures including frequency (daily, weekly, monthly) and scope (full backup, incremental backup, differential backup).

- Coverage of backup procedures (e.g., hard disk on servers only, client and server hard disks).

- Location of stored backups (off-site or on-site).

- Generations of backups kept.

III.E.3.d. Audit and Variance Detection

Audit and variance detection controls allow management to conduct an independent review of records and activities to test the adequacy of system and application controls and to detect and react to departures from established policies, rules, and procedures. Variance detection includes the use of system logs and audit trails. For an application, variance detection checks for anomalies in user or system behavior, in such things as the numbers and types of transactions, volume and dollar thresholds, access outside normal work hours and other deviations from standard activity profiles. These reviews may provide early detection of unauthorized system or application access attempts as well as contaminated software (erroneous or malicious programs or computer viruses).

Two basic types of reviews fit into this category of controls—system audits and security monitoring:

- System audits are “snapshot” analyses of applications at a specific point in time. Audits can be self-administered or independent (either internal or external). System audits may be independent or performed by internal staff. Independent audits provide less bias while internal audits allow for more ongoing analysis of system operations. Independent audits may be performed by individuals from other parts of the organization (e.g., Inspector General’s Office, agency Computer Security Program Manager) or external organizations (contractors, General Accounting Office). For large, highly vulnerable applications, such as financial applications, hiring a professional external organization to perform a security audit may be justified.

- Security monitoring is an ongoing activity that is intended to identify vulnerabilities, deviations from established security procedures, and other security concerns. Monitoring is similar to system audits in that many of the same analytical procedures are used. System monitoring, however, is performed more regularly and is more likely to identify minor or transitory events that may be indicative of potential security intrusions, threats, or weaknesses. System monitoring tools are typically used to assist security monitoring tools for “real time” analysis.

In this section, describe the system monitoring procedures (including scope and frequency) and the process for resolving any concerns identified. List and describe any system audits, internal reviews, or other audits performed. Include in this discussion the following items:

- Who conducted the audit?

- When was the audit conducted?

- What methodology was used (checklists, penetration tests, transaction analysis, audit trail analysis)?

- What were the audit findings? and

- What has been done to resolve audit findings?

If this information is included in other sections of the plan (i.e., Sections II.B, III.E.2.a., III.E.2.c.), provide a reference to the section where it is contained.

III.E.3.e. Application Software Maintenance Controls

These controls are used to monitor the installation of, and updates to, application software to ensure that the software functions as expected and that a historical record is maintained of application changes. This helps ensure that only authorized software is installed on the system. Such controls may include a software configuration policy that grants managerial approval (re-certification and re-accreditation) to modifications and requires that changes be documented. Other controls include products and procedures used in auditing for, or preventing illegal use of shareware or copyrighted software. Software maintenance procedures may also be termed version control, change management, or configuration management. The following questions are examples of items that should be addressed in responding to this section:

- Was the application software developed in house or under contract?

- Does the Government own the software?

- Was the application software received from another Federal agency with the understanding that it is Federal Government property?

- Is the application software a copyrighted commercial off-the-self product or shareware?

- If a copyrighted commercial off-the-self product (or shareware), were sufficient licensed copies of the software purchased for all of the systems on which this application will be processed?

- Is there a formal change control process in place for the application, and if so, does it require that all changes to the application software be tested and approved before being put into production?

- Are test data “live” data or made-up data?

- Are all changes to the application software documented?

- Are test results documented?

- How are emergency “fixes” handled?

- Are there organizational policies against illegal use of copyrighted software or shareware?

  - Do the policies contain provisions for individual and management responsibilities and accountability, including penalties?

  - Are periodic audits conducted of users’ computers (PCs) to ensure only legal licensed copies of software are installed?

  - What products and procedures are used to protect against illegal use of software?

- Are software warranties managed to minimize the cost of upgrades and cost-reimbursement or replacement for deficiencies?

III.E.3.f. Documentation

Documentation is a security control in that it explains how software/hardware is to be used and formalizes security and operational procedures specific to the system. Documentation for a system includes descriptions of the hardware and software, policies, standards, procedures, and approvals related to automated information system security in the application and the support system(s) on which it is processed, to include backup and contingency activities, as well as descriptions of user and operator procedures.

Documentation should be coordinated with the general support system and/or network manager(s) to ensure that adequate application and installation documentation are maintained to provide continuity of operations. List the documentation maintained for the application.

The example list is provided to show the type of documentation that would normally be maintained for a system and is not intended to be all inclusive or imply that all systems should have all items listed

Example Documentation for Major Application

- Vendor supplied documentation of hardware
- Vendor supplied documentation of software
- Application requirements
- Application Security Plan
- General support system(s) security plan(s)
- Application program documentation and specifications
- Testing procedures and results
- Standard operating procedures
- Emergency procedures
- Contingency plans
- Memorandums of understanding with interfacing systems
- Disaster recovery plans
- User rules/procedures
- User manuals
- Risk assessment
- Backup procedures
- Certification documents and statements
- Accreditation statements

This page intentionally blank.

III.E.4. SECURITY AWARENESS AND TRAINING

The Computer Security Act requires Federal agencies to provide for the mandatory periodic training in computer security awareness and accepted computer security practice of all employees who are involved with the management, use, or operation of a Federal computer system within or under the supervision of the Federal agency. This includes contractors as well as employees of the agency. OMB Circular A-130, Appendix III, issued in 1996, enforces such mandatory training by requiring its completion prior to granting access to the system and through periodic refresher training for continued access. Therefore, each user should be versed in acceptable behavior — the rules of the system — before being allowed to use the system. Training should also inform the individual how to get help in the event of difficulty with using the system, and inform them of security incident and reporting procedures for the system.

In addition to training related to the rules of the general support system, users must also receive specialized training focused on their responsibilities and rules for any applications before access. Access provided to members of the public should be constrained by controls in the applications, and training should be within the context of those controls and may consist only of notification at the time of access.

III.E.4.a. Security Awareness and Training Measures

All employees and contractors involved with the management, use, design, development, maintenance or operations of the application should be aware of their security responsibilities and trained in how to fulfill them. Include the information about the following in this section of the plan:

- The awareness program for the system (posters, booklets, trinkets).

- The type and frequency of application specific training provided to employees and contractor personnel (seminars, workshops, formal classroom, focus groups, role-based training, on-the-job training).

- The type and frequency of general support system training provided to employees and contractor personnel (seminars, workshops, formal classroom, focus groups, role-based training, on-the-job training).

- The nature of system security awareness provided during new employee orientation.

- The procedures for assuring that employees and contractor personnel have been provided adequate training.

Note: Contractor employees are required to receive the same level of automated information systems security awareness and training as Federal employees. This training requirement should be included as appropriate in all contracts.

This page intentionally blank.

III.E.5. TECHNICAL CONTROLS

Technical controls are hardware and software controls used to provide automated protection from unauthorized access or misuse, to facilitate detection of security violations, and support security requirements for applications and data. Normally these types of controls are coordinated with the network and/or general support system managers.

Although the following controls are not addressed in detail in the OMB Circular A-130, Appendix III, updated in 1996, the Circular states that “the technical security controls defined in OMB Bulletin No. 90-08 will continue.” To satisfy this requirement, and address the continuing importance of technical controls and their role in protection for all systems, the controls described below are incorporated from OMB Bulletin 90-08.

III.E.5.a. User Identification and Authentication

These are controls used to verify the identity of a station, originator, or individual prior to allowing access to the system, or specific categories of information within the system. Such controls may also be used to verify that only authorized persons are performing certain processing activities on the system. These controls include the use of passwords, tokens, or biometrics or other personal mechanisms to authenticate an identity.

User authentication is based on three categories of information: something the user knows, such as password; something the user possesses, such as a token; and some physical characteristic (biometrics) of the user, such as a fingerprint.

The most common type of authentication mechanism is the password. Password use became popular because passwords are easy to implement and provide a reasonable degree of authentication.

One of the weaknesses in using passwords to control access to systems and applications is the possibility of an individual user’s password being guessed. If users change their own passwords, they frequently select a password that is easy for them to remember (e.g., common word, name or date associated with a family member, sports-related word, or a repeat of their user identification [ID]). Software programs are available that are designed to be “password crackers.” These “password crackers” check passwords against dictionaries and other criteria for easy-to-guess passwords and provide reports that can be used to motivate users to change their passwords to something more secure.

WARNING: Many computer systems and software programs are shipped with administrative accounts that have preset default passwords. Because these passwords are standard, they are widely known. System Administrators frequently do not change these default passwords, creating a significant vulnerability for the system and any applications it supports.

Given the broader nature of system threats and increased use of IT to support mission-critical functions, more stringent authentication mechanisms (as stand alone controls or in combination with passwords) may be appropriate. Authentication methods employing a token or biometrics can provide a significantly higher level of security than passwords alone. Cryptography is often incorporated into advanced authentication systems, such as those using token or biometric methods.

Password systems, if structured properly, can provide several levels of controls, with assurances that only authorized users access the system or applications.   Proper password structure meets the criteria from NIST FIPS 112, “Standard on Password Usage,” which is a mandatory standard for all Federal agencies. If the system uses additional levels of passwords for the applications, for each control below, as appropriate, provide the requested information. Include information for both the general support system and applications in the security plan, as appropriate.

In this section, describe the system’s access controls. The description should include consideration for the following items:

- Describe the method of user authentication (password, token, biometric).

- If a password system is used, provide the following specific information:

    - Allowable character set,
    - Password length (minimum, maximum),
    - Password aging time frames and enforcement approach,
    - Number of generations of expired passwords disallowed for use,
    - Procedures for password changes,
    - Procedures for handling lost passwords, and
    - Procedures for handling password compromise.
    - Procedures for training users and the materials covered.

Note: The recommended minimum number is six to eight characters in a combination of alpha, numeric, or special characters.

- Indicate the frequency of password changes, describe how password changes are enforced (e.g., by the software or System Administrator), and identify who changes the passwords (the user, the system, or the System Administrator).

- Describe any biometric controls used. Include a description of how the biometric controls are implemented on the system.

- Describe any token controls used on this system and how they are implemented.
  - Are special hardware readers required?
  - Are users required to use a unique Personal Identification Number (PIN)?
  - Who selects the PIN, the user or System Administrator?
  - Does the token use a password generator to create a one-time password?
  - Is a challenge-response protocol used to create a one-time password?

- Describe the level of enforcement of the access control mechanism (network, operating system, application).

- Describe how the access control mechanism supports individual accountability and audit trails (e.g., passwords are associated with a user identifier that is assigned to a single individual).

- Describe the self-protection techniques for the user authentication mechanism (e.g., passwords are stored with one-way encryption to prevent anyone [including the System Administrator] from reading the clear text passwords, passwords are automatically generated, passwords are checked against a dictionary of disallowed passwords, passwords are encrypted while in transmission).

- State the number of invalid access attempts that may occur for a given user identifier or access location (terminal or port) and describe the actions taken when that limit is exceeded.

- Describe the procedures for verifying that all system-provided administrative default passwords have been changed.

- Describe the procedures for limiting access scripts with embedded passwords (e.g., scripts with embedded passwords are prohibited, scripts with embedded passwords are only allowed for batch applications).

- Describe any policies that provide for bypassing user authentication requirements, single-sign-on technologies (e.g., host-to-host, authentication servers, user-to-host identifier, group user identifiers) and any compensating controls.

III.E.5.b. Authorization/Access Controls

Describe hardware or software features that are designed to permit only authorized access to or within the application, to restrict users to authorized transactions and functions, and/or to detect unauthorized activities (e.g., access control lists).

Logical Access Controls

Computer system-based access control, or logical access control, is the mechanism used to specify “who” (subjects) can do “what” to resources controlled by the system or application (objects). Typical access modes are read, write, create, modify, execute programs, and delete data, programs and files. Access control safeguards also control the ability to access and use other system resources, such as external networks or communications, utility programs, or the computer operating system. Access control is discretionary when users can delegate access permissions to other users. This can be done directly by establishing access control lists or indirectly, by copying a file to a public area on the system. In this section, discuss the controls in place to authorize or restrict the activities of users and ADP personnel within the application.

- Describe formal policies that define the authority that will be granted to each user, or class of users. Indicate if these policies follow the concept of “least privilege” which requires identifying the user’s job functions, determining the minimum set of privileges required to perform that function, and restricting the user to a domain with those privileges and nothing more.

- Identify whether the policies include “separation of duties” enforcement to prevent an individual from having all necessary authority or information access to allow fraudulent activity without collusion.

- Describe the application’s capability to establish an Access Control List, or register of the users and the types of access they are permitted.

- Indicate whether a manual Access Control List is maintained.

- Indicate if the security software allows application owners to restrict the access rights of other application users, the general support system administrator, or operators to the application programs, data, or files.

- Describe how application users are restricted from accessing the operating system, other applications, or other system resources not needed in the performance of their duties.

- Describe any formal process requiring application owners to authorize all new users and define their individual rights or restrictions to read, write, create, modify, execute application programs, or delete application data or files.

- When the role or job function of a user changes, describe any formal process to review the access authorizations and change any rights or restrictions in line with the new requirements.

Note: It is particularly important that any rights no longer required for job performance be removed. Users will usually complain if restrictions prevent them from doing what they need to do, but rarely ask to have privileges taken away, even if they no longer need them.

- Indicate how often Access Control Lists are reviewed to identify and remove users who have left the organization or whose duties no longer require access to the application.

- Describe controls to detect unauthorized transaction attempts by authorized and/or unauthorized users.

- Describe policy or logical access controls that regulate how users may delegate access permissions or make copies of files or information accessible to other users. This "discretionary access control" may be appropriate for some applications, and inappropriate for others. Document any evaluation made to justify/support use of "discretionary access control."

- Indicate after what period of user inactivity the system automatically blanks associated display screens and/or after what period of user inactivity the system automatically disconnects inactive users or requires the user to enter a unique password before reconnecting to the system or application.

- Describe any restrictions to prevent users from accessing the system or applications outside of normal work hours or on weekends. Discuss in-place restrictions.

- Indicate if encryption is used to prevent unauthorized access to sensitive files as part of the system or application access control procedures. (If encryption is used primarily for confidentiality or integrity controls, include this information in the appropriate section.) If encryption is used as part of the access controls, provide information about the following:

    - What cryptographic methodology (e.g., secret key, public key) is used? If a specific off-the-shelf product is used provide the name of the product. If it meets Federal standards (e.g., Data Encryption Standard, Digital Signature Standard), include that information.

    - Discuss cryptographic key management procedures for key generation, distribution, storage, entry, use, destruction, and archiving.

Remote Users

Describe the type of remote access (dial, Internet) permitted and the functions that may be authorized for remote use (e-mail only, data retrieval only, full access). The following are some of the issues that should be addressed in this description:

Dial-In Access

- Document whether the system disconnects after a set number of improper password attempts, and describe any controls to prevent a person from re-dialing and trying additional passwords.

- Document who has access through the dial-in lines (by user type and number of users).

- Describe the procedures for obtaining the telephone numbers for dial-in lines, including controls to prevent unauthorized individuals from dialing in (e.g., the dial-in telephone numbers are unpublished and/or unlisted). If dial-in telephone numbers are published, describe why, where, and how extensively.

- Document whether the system/application has a dial-back capability.

Wide Area Networks

If your application is running on a system that is connected to the Internet or other wide area network(s), discuss what additional hardware or technical controls have been installed and implemented to provide protection against unauthorized system penetration and other known Internet threats and vulnerabilities.

- List the connections to the Internet or other wide area networks, including whether application users access the system through the Internet or a wide area network.

- Describe any type of secure gateway or firewall in use, including its configuration, (e.g., configured to restrict access to critical system resources and to disallow certain types of traffic to pass through to the system).

- Provide information regarding any port protection devices used to require specific access authorization to the communication ports, including the configuration of the port protection devices and if additional passwords or tokens are required.

- Identify whether internal security labels are used to control access to specific information types or files, and if such labels specify protective measures or indicate additional handling instructions.

- Indicate if host-based authentication is used. (This is an access control approach that grants access based on the identity of the host originating the request, instead of the individual user requesting access.)

Screen Warning Banners

Systems with external communications may need to alert potential users that inappropriate use may be subject to prosecution. Public Law 99-474 requires that a warning message be displayed, notifying unauthorized users that they have accessed a U.S. Government computer system and unauthorized use can be punished by fines or imprisonment. Although, the warning does not prevent unauthorized use of the system, it does facilitate prosecution of violators (i.e., failure to notify an unauthorized user that it is a Government system may make prosecution more difficult, regardless of how much damage is done to the system).

Some of the systems now in use are intended for unrestricted use by the general public (e.g., Internet-based systems used for widespread public information dissemination), a situation not prevalent when P.L. 99-474 was enacted. Thus, due to their adverse impact on the intended user population, highly restrictive warning banners may not be appropriate. The choice of which screen warning banner to implement is up to the system owner and should be based on system specific technology limitations, data sensitivity, or other unique system requirements. In this section describe the rationale for electing to use or not use warning banners and provide an example of the banners used. Where appropriate, state whether the warning banner was approved by the Department of Justice, Computer Crime Unit.

Don't Forget

System opening banners/messages that include the word "Welcome" in log-in sequence the may be interpreted to authorize the use of the system by anyone. Such interpretations are not appropriate for systems restricted to access by pre-authorized Government users. If access to your system is limited to Government users (including contractors and other pre-authorized individuals) and your banner includes the word "Welcome" it should be removed to allow easier prosecution of unauthorized users.

Example Warning Banners

Banner	Selection Rationale	Approved by DOJ Computer Crime Unit
WARNINGWARNING**WARNING** This is a (Agency) computer system. (Agency) computer systems are provided for the processing of Official U.S. Government information only. All data contained on (Agency) computer systems is owned by the (Agency) *may be monitored, intercepted, recorded, read, copied, or captured in any manner and disclosed in any manner*, by authorized personnel. THERE IS NO RIGHT OF PRIVACY IN THIS SYSTEM. System personnel may give to law enforcement officials any potential evidence of crime found on (Agency) computer systems. *USE OF THIS SYSTEM BY ANY USER, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO THIS MONITORING, INTERCEPTION, RECORDING, READING, COPYING, OR CAPTURING and DISCLOSURE.* **WARNING**WARNING**WARNING**	System is for Government use only and all transmissions may be monitored.	Yes
WARNINGWARNING**WARNING** This is a United States (Agency) computer system, which may be accessed and used only for official Government business by authorized personnel. Unauthorized access or use of this computer system may subject violators to criminal, civil, and/or administrative action. All information on this computer system may be intercepted, recorded, read, copied, and disclosed by and to authorized personnel for official purposes, including criminal investigations. Access or use of this computer system by any person whether authorized or unauthorized, constitutes consent to these terms. **WARNING**WARNING**WARNING**	System is for Government use only. Monitoring is only performed in support of system operations and to investigate potential security events.	Yes
The seals, initials, and agency identification can not be used without the written permission of the agency.	Information dissemination system open to the general public. Associated risks are denial of access and transitory embarrassment to the agency.	No
None	Information dissemination system open to the general public. Associated risks are denial of access and transitory embarrasment to the agency.	No

III.E.5.c. Public Access Controls

Where an agency's application promotes or permits public access, additional security controls are needed to protect the integrity of the application and the confidence the public has in the application. Such controls include segregating information made directly accessible to the public from official agency records.

Public access systems are subject to a greater threat from outside attacks. In public access systems users are often anonymous and untrained in the system and their responsibilities. Attacks on public access systems could have a substantial impact on the organization's reputation and the level of public trust and confidence. Threats from insiders are also greater (e.g., errors introduced by disgruntled employees or unintentional errors by untrained users).

The following list contains some controls that might provide protection in a public access system. It is not intended to include all possible controls or imply that all systems should have all controls listed.

If this is a public access system, list and discuss the controls that provide protection to the system.

Example Public Access Controls

- Some form of identification and authentication (this may be difficult)
- Access control to limit what the user can read, write, modify, or delete.
- Controls to prevent public users from modifying information on the system
- Digital signatures
- CD-ROM for on-line storage of information for distribution
- Put copies of information for public access on a separate system
- Prohibit public to access "live" databases
- Verify that programs and information distributed to the public are virus-free
- Audit trails

III.E.5.d. Data Integrity/Validation Controls

Data integrity controls are used to protect data from accidental or malicious alteration or destruction and to provide assurance to the user that the information meets expectations about its quality and that it has not been altered. Validation controls refer to tests and evaluations used to determine compliance with security specifications and requirements.

Integrity is a quality of information that is based on the attributes of accuracy, timeliness, and completeness. System integrity is the quality of a system/software process that ensures that it does what it is supposed to do and nothing more.

Discuss any controls to provide assurance to users that the information has not been altered and that the system functions as expected. Include any tests or evaluations that were used to determine compliance with security requirements during development or modification. Some of the controls that fit in this category include:

Malicious Programs

In this section, provide a brief overview and reference the items in the discussion of configuration management and personnel controls that describe control measures intended to prevent installation of software that performs unauthorized functions.

Virus Protection

One of the most significant controls for smaller systems, including file servers, is virus detection and elimination software. It may also be appropriate to install this type of software on secure gateways, depending on the threat. Virus detection/ elimination software could cause a slow down of data transfer. In this section describe the virus detection/elimination approach used for the system. Include in this discussion the following items:

- A list of components on which virus detection software is installed (client, server, firewall) and a rationale for its use. Also include a statement as to whether the license is current.

- Procedures for updating virus signature files.

- Procedures for automatic and/or manual virus scans (automatic scan on network log-in, automatic scan on client/server power on, automatic scan on diskette insertion, automatic scan on download from an unprotected source such as the Internet, scan for macro viruses).

- Virus eradication and reporting procedures.

- Virus eradication support availability (e.g., central technical support specialists, incident response capability).

Message Authentication

Message authentication is a method using cryptographic approaches to ensure that the sender of a message is known and that the message has not been altered during transmission. State whether message authentication has been determined to be appropriate for your system.

If message authentication is used, describe the methodology.

Integrity Verification

Integrity verification programs can be used by applications to look for evidence of data tampering, errors, and omissions. Techniques include consistency and reasonableness checks and validation during data entry and processing. These techniques can check data elements, as input or as processed, against expected values or ranges of values. Message authentication techniques may also be used to ensure data integrity while in transit or storage.

Describe the integrity controls used within this system.

Reconciliation

Reconciliation routines use checksums, “hash totals,” record counts, and other approaches to detect unauthorized changes to data and/or program files. These approaches generate a mathematical value based on the contents of a particular file which is stored external to the file. To verify the integrity of the file, the mathematical value is recomputed on the current file and compared with the previously generated value. The two values should match.

Describe any reconciliation routines used by the system. Include a description of the actions taken to resolve any discrepancies.

Digital Signature

Digital signatures provide an extremely high level of integrity assurance. Federal agencies using digital signatures must use technology that conforms with FIPS 186, “Digital Signature Standard” and FIPS 180, “Secure Hash Standard” issued by NIST, unless a waiver has been granted. Digital signatures provide assurance of the identity of the originator, that the originator cannot falsely deny having signed the file (non repudiation), that the file has not been modified after being signed, and that the originator intends to be bound by the contents of the file. Digital signatures are designed to meet the standards of proof required by law. Digital signatures are required to replace a hand-written signature on a commitment document (e.g., contract, funds transfer document) or if the results of a risk analysis shows that level of protection is necessary and cost-effective.

Electronic signatures that meet some, but not all of the digital signature standard may also be used to provide lower levels of integrity control. For most systems, these less secure “electronic signatures” may be adequate integrity protection.

In this section describe any use of digital or electronic signatures. Address the following specific issues:

- State the digital signature standards used. If the standards used are not NIST standards, please state the date the waiver was granted and the name and title of the official granting the waiver.

- Describe the use of electronic signatures and the security control provided.

- Discuss cryptographic key management procedures for key generation, distribution, storage, entry, use, destruction and archiving.

III.E.5.e. Audit Trail Mechanisms

Audit trail mechanisms are controls that provide a system monitoring and recording capability to retain a chronological record of system activities. Audit trails enable reconstruction of a transaction from its inception to final results—including any modification of files. One type of audit trail, keystroke monitoring, is usually used to protect systems from intruders who access the system without authority or in excess of their assigned authority. Section III.E.5.b. contains information about screen warning banners required on systems with keystroke monitoring capability.

Other audit trails are event-oriented and include system, application, and user audit capability. System audit trails are generally used to monitor and fine-tune system performance. They should be able to record all log-on attempts, user identification, date/time, devices used, functions performed, applications accessed and user log-off, but may not be able to log events within applications. Application audit trails may be used to detect flaws in applications, or violations of security policy committed with an application. User audit records are generally used to hold individuals accountable for their actions. An audit trail should include sufficient information to establish what events occurred, when they occured, and who caused them (i.e., the associated user identifier).

No matter how much information is captured by the audit trail, it serves no purpose unless it is routinely monitored for unusual activity (e.g., violations of policy or rules of behavior or unauthorized access attempts). Reviews include —

- Regularly scheduled analysis of audit trail reports by system and application owners or automated information system security personnel.

- Special reviews after the occurrence of an unanticipated event.

- Real-time audit analysis by automated audit tools with manual follow-up of identified anomalies.

Access to on-line logs or audit reports must be strictly controlled to prevent destruction or modification of the records. Audit trail records may be used as legal evidence and protecting their integrity is critical. In addition, audit trails may record information about individual user activities which must be protected for confidentiality. Audit trail records should be protected by strong access controls to help prevent unauthorized access. The use of encryption and digital signatures may also be considered for audit logs of very sensitive applications.

In this section, describe the measures used to protect system usage and audit trail logs. Include consideration for the following items in this discussion:

- List the system usage and audit trail logs (including the events logged and data elements recorded) produced by the general support system.

- Describe any linkages between logs maintained by the system and the supported applications.

- Describe how the actions of individual users of the system may be monitored through the system logs.

- Describe procedures used for reviewing logs and audit trail reports.

This page intentionally blank.

III.E.6. COMPLEMENTARY CONTROLS PROVIDED BY SUPPORT SYSTEMS

The application owner for the application should understand and accept the risk inherent in processing on the network or at the installation(s) that support the application, particularly where the support system is operated outside of their management control (e.g., by another organization). If not, plans for greater understanding of that risk should be described.

- List any controls in place on the general support system that add protection for the application.

- If the application is processed on another system(s), include the name of the organization, system name, and if one exists, its unique system identification.

- Indicate how the application owner has acknowledged understanding of the risk to application information that is inherent in processing on the general support system or in transmitting information over networks.

Application owners should ask the general support system for the types of controls in place. This may necessitate a review of the security plan(s) for the general support system(s). If the security is not adequate for protection of the application information, the application owner should request additional levels of security controls.

It is the responsibility of the application owner to provide information to the general support system about the security controls required to protect application information. The general support system has no responsibility to provide security beyond its own system protection levels, unless an agreement has been made with the application owner for additional controls. If a general support system can not or will not provide security adequate for the application, it is the responsibility of the application owner to implement additional controls or seek alternate processing capability.

This page intentionally blank.

IV. ADDITIONAL COMMENTS

This section provides an opportunity to include additional comments about the security of the subject system and any perceived need for guidance or standards. Use this section to discuss any features or administrative standards that are in place within your environment that may not be covered in the rest of the plan. Also, include information in this section about planned major changes that might affect this application in the future (e.g., this application will be replaced during the third quarter of FY98 by a new application being developed, this application is to be combined with other applications, other Federal agencies will be accessing and using this application in January 1999, or data from this application will be used to produce data in a separate system for public access within the next year). Include discussion of any Federal or organizational security policies, standards, or guidelines that apply.

This page intentionally blank.

FORMAT 2 — GENERAL SUPPORT SYSTEMS

Don't Forget

Note: If the system is identified as a **general support system** in Section I.C., *System Category*, use this format. If the system is identified as a **major application**, use Format 1.

*Begin each of the following control sections by indicating the appropriate "Security Control Measure Status" — **"In-Place," "Planned," "In-Place and Planned,"** or **"Not Applicable"** before discussing the control information. For sections where some controls are **"In-Place"** while others are **"Planned"** list or discuss each category separately, and remember to include milestone dates for completion of the planned actions.*

III.E.1. MANAGEMENT CONTROLS

Describe the overall management controls of the general support system.

III.E.1.a. Assignment of Security Responsibility

For each general support system, an individual should be assigned in writing as the focal point for assuring that security is adequate within the system, including methods used to prevent, detect, and recover from security events. The individual assigned should be trained in the technology used in the system and in the security management and control measures appropriate for that technology (e.g., user identification and authentication).

List the name, title, telephone number, and where available, e-mail address of the individual who has been assigned responsibility for the security of the system (i.e., the Automated Information System Security Officer - AISSO). Indicate whether the idividual has been designated in writing as the AISSO.

Example

Bill Smith, AISSO
Computer Specialist
ABC Division, XYZ Branch
1111 West Street, Room 444
Rockville, MD 20852
(301) 123-1213
Bill_Smith@agency.gov

III.E.1.b. Personnel Security

The greatest harm/disruption to a system comes from the actions of individuals, both intentional and unintentional. Often systems experience disruption, damage, loss, or other adverse impact due to the well-intentioned actions of individuals authorized to use or maintain a system (e.g., the programmer who inserts “one minor change” then installs the program into the production environment without testing). Personnel controls (technical, operational, and management) are intended to prevent the occurrence or minimize the impact of undesirable events caused by the actions of individuals (authorized as well as not authorized for system access). Such controls include individual accountability, least privilege, and separation of duties.

Individual accountability consists of holding individuals responsible for their actions. In a general support system, accountability is accomplished by identifying and authenticating individuals and providing the capability to associate them with their actions (install a new program, execute a program) relative to the system. This may be accomplished through user identifiers assigned to each individual, audit trails, and/or pattern analysis of system usage data.

Least privilege is the practice of restricting a user’s access (to data files, to processing capability, or to peripherals) and type of access (e.g., read, write, execute, delete) to the minimum necessary to perform his or her job.

Separation of duties is the practice of dividing the steps in a critical function among different individuals. For example, one system programmer can create a segment of operating system code, a manager authorizes its implementation, and the implementation is effected by a second system programmer. Such a control keeps a single individual from subverting a critical process or inserting that “one last minor change” without testing. Separation of duties may be enforced through administrative or technical controls.

Federal policies require that all automated data processing (ADP) positions be evaluated and a sensitivity level be assigned to the position description. A background investigation is required for all employees and contractors assigned to sensitive positions. The requirement for background screening includes both Government and contractor personnel who design, implement, maintain, or use the system. The type of background investigation required is determined by the sensitivity level assigned to the individual position description, the individual’s level of system responsibility and authority, and an assessment of the adequacy of the control environment.

In some instances, it may be necessary to authorize an individual to bypass significant technical and operational controls to perform system administration and maintenance functions (e.g., LAN administrators, systems programmers, system administrators). The number of such positions should be kept to the minimum necessary to support system requirements. Background screening of individuals in such positions of trust supplements technical, operational, and management controls. Background screening is particularly necessary where the risk and magnitude of harm is high and effectiveness of technical and administrative controls can not be assured.

Include detailed information about any personnel controls that are not included in other sections of this security plan, (i.e., technical controls and rules). Also include a short discussion or list of controls discussed in detail in other sections of the plan, or reference section numbers of this plan where detailed information is included. These discussions should include the following specific items:

- A statement as to whether all positions have been reviewed for sensitivity level. If all positions have not been reviewed, state the planned date for completion of position sensitivity analysis.

- A statement as to whether individuals have received the background screening appropriate for the position to which they are assigned. If all individuals have not had appropriate background screening, include the date by which such screening will be completed.

- If individuals are permitted system access prior to completion of appropriate background screening, describe the conditions under which this is allowed and any compensating controls to mitigate the associated risk.

This page intentionally blank.

III.E.2. ACQUISITION / DEVELOPMENT / INSTALLATION CONTROLS

Acquisition, development, and installation controls are the administrative procedures and technical controls used to ensure that adequate protection is built into the system during development and that the system only performs those functions authorized by management. The controls should define an on-going process to ensure continued operation at an acceptable level of risk during the installation, implementation, and operation and maintenance phases of the system.

III.E.2.a. Authorize Processing

Systems must have specific authorization to initiate and continue production operations. The authorization of a system to process information, granted by a senior management official, is an important quality control and is required by OMB Circular A-130. In this section of the plan, include the following information:

Certification: Date of certification, name and title of Certifying Official
If not certified, name and title of manager requesting approval to operate and date of request.

Accreditation: Date of approval to process/accreditation, name and title of individual approving/accrediting the system for processing.

If the general support system has not been certified or accredited, include reasonable milestone dates (month and year) for completing all requirements and obtaining certification and accreditation for the system.

<u>Approval to Process/Accreditation</u>

Some agencies refer to the process of granting systems approval to operate as accreditation. By approving/accrediting operation of a system, a manager—

- Accepts the associated risks to the organizational mission and assets (hardware, software, data); and

- States that there is reasonable assurance that system assets are adequately protected against waste, fraud, and abuse and that “the system does what it is supposed to do, and nothing more.”

Approval to operate is a decision that should be made by an individual with the authority to budget for and allocate resources to resolve concerns that create unacceptable risks. The position of this individual will vary between organizations. Approval to operate is not a decision that may be made by the security staff.

Both the security official and the approving management official have security responsibilities. The security official is closer to the day-to-day operation of the system and thus will direct, perform, or monitor security tasks. The approving official will have management responsibility for or within the organization supported by the system.

Management authorization should be based on an assessment of management, operational and technical controls. Since the security plan establishes the system protection requirements and documents the appropriate controls necessary to reach an acceptable level of risk, it forms the basis for the approval to operate, supplemented by specific studies as needed. In addition, the periodic review of controls should contribute to future decisions regarding the approval to operate.

Management approval/authorization to process should be granted prior to initial implementation and at least every three years thereafter or when there are major changes to the system. System approval decisions and the associated analyses should be performed more often where there is a high risk and potential magnitude of harm.

Some agencies have established the system approval process as a formal accreditation procedure where the approving authority is termed the Designated Approving/Accreditation Authority (DAA). Formalization of the system approval process reduces the potential that systems will be placed into a production environment without appropriate management review.

Certification Reviews

Prior to accreditation, each general support system should undergo a technical evaluation to ensure that—

- It meets applicable Federal laws, regulations, policies, guidelines, and standards;

- In-place and planned security safeguards appear to be adequate and appropriate for the system; and

- In-place safeguards are operating as intended.

These technical reviews are generally termed “certification reviews” and are often independent reviews. Certification reviews are intended to provide a technical analysis of system controls and other security arrangements in support of a management decision as to whether an “authorization to process” should be granted (e.g., the system is accredited for processing). Technical certification reviews (such as those using the methodology in FIPS Publication 102 “Guidelines for Computer Security

Certification and Accreditation") provide useful information to assist management in authorizing a system, particularly when combined with a review of the broad behavioral controls envisioned in the security plan, as required by OMB Circular A-130.

In some agencies, a certification review includes a specific system test and evaluation (ST&E). The ST&E is a formal test of the system and its associated controls to ensure that in place controls are functioning.

Some agencies have established formal certification procedures that require that systems must be "certified" before they may be submitted for an approval to operate decision. In these cases, a management official with a technical background typically acts as the Certifying Official. The Certifying Official issues a certification statement and prepares and forwards an approval/accreditation package to the individual designated as the approving official or DAA requesting formal approval to process for the system.

III.E.2.b. Acquisition Specifications

Appropriate technical, administrative, physical, and personnel security requirements are to be included in specifications for the acquisition or operation of information technology installations, equipment, software, and related services. As changes occur that affect the system, the specifications will need to be updated to reflect new requirements. Address the following in the security plan:

- Development of security requirements with associated evaluation and test procedures before the procurement action(s).

- Inclusion of security requirements and evaluation/test procedures in appropriate solicitation documents (e.g., Requests for Proposals).

- Inclusion of provisions that permit updating security requirements as new threats/vulnerabilities are identified and as new technologies are implemented.

Include a general discussion of security specifications used, how they relate to specific system requirements, and whether the security specifications were reviewed and approved by the appropriate security personnel.

This page intentionally blank.

III.E.3. OPERATIONAL CONTROLS

Operational controls are the day-to-day procedures and mechanisms used to protect production general support systems (or planned systems when they become operational). Operational controls affect the system and application environments.

III.E.3.a. Physical and Environmental Protection

Discuss the controls used to protect against the wide variety of physical and environmental threats and hazards that could affect the system, including deliberate intrusions, natural or man-made hazards, and utility outages or breakdowns (e.g., computer room locks, surge suppressors, special fire fighting equipment, "hardened" communications).

Appropriate and adequate controls will vary depending on the individual system requirements. The example list shows the types of controls in this category. The list is not intended to be all inclusive or to imply that all systems should have all controls listed.

Example Physical/Environmental Controls

In Place

- Card keys for building and work area entrances
- 24-hour guards at all entrances/exits
- Cipher lock on computer room door
- Raised floor in computer room
- Dedicated cooling system
- Humidifier in tape library
- Emergency lighting in computer room
- Four fire extinguishers rated for electrical fires
- One B/C rated fire extinguisher
- Smoke, water, and heat detectors
- Emergency power-off switch by exit door
- Surge suppressor
- Emergency replacement server
- Zoned dry pipe sprinkler system
- Uninterruptable power supply for LAN servers
- Power strips/suppressors for peripherals
- Power strips/suppressors for computers
- Controlled access to file server room

Planned

- Plastic sheets for water protection, August 1997
- Closed-circuit television monitors, January 1998

III.E.3.b. Production, Input/Output Controls

Discuss controls over the marking, handling, processing, storage, and disposal of input and output information and media, as well as access controls (such as labeling and distribution procedures) for the information and media. The discussion should include consideration of the following:

- Procedures to ensure unauthorized individuals cannot read, copy, alter, or steal printed or electronic information.
- Procedures for ensuring that only authorized users pick up, receive, or deliver input and output information and media.
- Audit trails for receipt of sensitive inputs/outputs.
- Procedures for restricting access to output products.
- Procedures and controls used for transporting or mailing media or printed output.
- Internal/external labeling for appropriate sensitivity (e.g., Privacy Act, Proprietary, Confidential, Secret).
- External labeling with special handling instructions (e.g., log/inventory identifiers, controlled access, special storage instructions, release or destruction dates).
- Audit trails for inventory management.
- Media storage vault or library physical and environmental protection controls and procedures.
- Procedures for sanitizing electronic media for reuse (e.g., overwrite or degaussing of electronic media).
- Procedures for controlled storage, handling, or destruction of spoiled media or media that can not be effectively sanitized for reuse.
- Procedures for shredding or other destructive measures for hardcopy media when no longer required.

III.E.3.c. Contingency Planning

General support systems require appropriate emergency, backup, and contingency plans. These plans should be tested regularly to assure the continuity of support in the event of system failure. Also, these plans should be known to users and coordinated with their plans for applications.

Describe the procedures (contingency plan) that would be followed to ensure the system continues to process all critical applications if a disaster should occur and provide a reference to the detailed plans. Include consideration of the following questions in this description:

- Are tested contingency plans in place to permit continuity of mission-critical functions in the event of a catastrophic event?

- Do the contingency plans for this system include all applications or do they have their own contingency plans?

- Are formal written emergency operating procedures posted or located to facilitate their use in emergency situations?

- How often are contingency, disaster, and emergency plans tested?

- Are all employees trained in their roles and responsibilities relative to the emergency, disaster, and contingency plans?

Include descriptions of the following controls.

- Any agreements for backup processing (e.g., hotsite contract with a commercial service provider).

- Documented backup procedures including frequency (daily, weekly, monthly) and scope (full backup, incremental backup, differential backup).

- Coverage of backup procedures (e.g., hard disk on servers only, client and server hard disks).

- Location of stored backups (off-site or on-site).

- Generations of backups kept.

III.E.3.d. Audit and Variance Detection

Audit and variance detection controls allow management to conduct an independent review of system records and activities to test for adequacy of system and application controls and to detect and react to departures from established policies, rules, and procedures. Variance detection includes the use of system logs and audit trails to identify anomalies in user or system behavior, in such things as the number of system accesses, types of accesses, and files accessed by users. These reviews may provide early detection of unauthorized system or application access attempts.

Two basic types of reviews fit into this category of controls—system audits and security monitoring:

- System audits are “snapshot” analyses of systems at a specific point in time. Audits can be self-administered or independent (either internal or external). System audits may be independent or performed by internal staff. Independent audits provide less bias while internal audits allow for more ongoing analysis of system operations. Independent audits may be performed by individuals from other parts of the organization (e.g., Inspector General’s Office, agency Computer Security Program Manager) or external organizations (contractors, General Accounting Office).

- Security monitoring is an ongoing activity that is intended to identify vulnerabilities, deviations from established security procedures, and other security concerns. Monitoring is similar to system audits in that many of the same analytical procedures are used. System monitoring, however, is performed more regularly and is more likely to identify minor or transitory events that may be indicative of potential security intrusions, threats, or weaknesses. System monitoring tools are typically used to assist security monitoring tools for “real time” analysis.

In this section, describe the system monitoring procedures (including scope and frequency) and the process for resolving any concerns identified. List and describe any system audits, internal reviews, or other audits performed. Include in this discussion the following items:

- Who conducted the audit?

- When was the audit conducted?

- What methodology was used (checklists, penetration tests, transaction analysis, audit trail analysis)?

- What were the audit findings? and

- What has been done to resolve audit findings?

If this information is included in other sections of the plan (i.e., Sections II.B, III.E.2.a., III.E.2.b.), provide a reference to the section where it is contained.

III.E.3.e. Hardware and System Software Maintenance Controls

Hardware and System Software Maintenance controls are used to monitor the installation and updates to hardware, operating system software, and other system software to ensure that the hardware and software functions as expected and that a historical record is maintained of system changes. These controls may also be used to ensure that only authorized software is allowed on the system. Potential controls include a hardware and system software configuration policy that grants managerial approval (re-certification and re-accreditation) to modifications and documents the changes. Other controls include products and procedures useful in auditing for, or preventing, illegal use of shareware or copyrighted software.

Routine Maintenance and Repair Service

All systems require periodic and emergency maintenance. Maintenance may be to upgrade or enhance system functionality or to effect repairs when the system no longer operates within established parameters. Procedures should be in place to ensure that maintenance and repair activities are accomplished without adversely affecting system security. In this section, describe the procedures for managing routine and emergency system maintenance and repair activities. Include in this discussion consideration for the following items:

- Restriction/controls on those who perform maintenance and repair activities.

- Special procedures for performance of emergency repair and maintenance.

- Management of hardware/software warranties and upgrade policies to maximize use of such items to minimize costs.

- Procedures used for items serviced through on-site and off-site maintenance (e.g., escort of maintenance personnel, sanitization of devices removed from the site).

- Procedures used for controlling remote maintenance services where diagnostic procedures or maintenance is performed through telecommunications arrangements.

Configuration Management/Change Control

Configuration management is a process for managing system changes. Configuration management allows the status of a system and its components to be identified at any point in time and ensures that only approved and tested changes are promoted to the production environment.

In this section, describe the configuration management procedures for the system. Include consideration for the following items in this discussion:

- Version control that allows association of system components to the appropriate system version.

- Procedures for testing and/or approving system components (operating system, other system, utility, applications) prior to promotion to production.

- Impact analyses to determine the effect of proposed changes on existing security controls.

- Change identification, approval, and documentation procedures.

- Procedures for ensuring contingency plans and other associated documentation are updated to reflect system changes.

Software Management

Describe the policies for handling copyrighted software or shareware. Include in this discussion consideration of answers to the following questions:

- Are there organizational policies against illegal use of copyrighted software or shareware?

  - Do the policies contain provisions for individual and management responsibilities and accountability, including penalties?

  - Are periodic audits conducted of users' computers (PCs) to ensure only legal licensed copies of software are installed?

  - What products and procedures are used to protect against illegal use of software?

- Are software warranties managed to minimize the cost of upgrades and cost-reimbursement or replacement for deficiencies?

III.E.3.f. Documentation

Documentation is a security control in that it explains how software/hardware is to be used and formalizes security and operational procedures specific to the system. Documentation for a system includes descriptions of the hardware and software, policies, standards, procedures, and approvals related to automated information system security on the support system, including backup and contingency activities, as well as descriptions of user and operator procedures.

The example list is provided to show the type of documentation that would normally be maintained for a system and is not intended to be all inclusive or imply that all systems should have all items listed.

Examples of General Support System Documentation

- Vendor supplied documentation of hardware
- Vendor supplied documentation of software
- General support system security plan
- Testing procedures and results
- Standard operating procedures
- Emergency procedures
- Contingency plans
- Disaster recovery plans
- User rules/procedures
- User manuals
- Risk assessment
- Backup procedures
- Certification documents and statements
- Accreditation statements

This page intentionally blank.

III.E.4. SECURITY AWARENESS AND TRAINING

The Computer Security Act requires Federal agencies to provide for the mandatory periodic training in computer security awareness and accepted computer security practice of all employees who are involved with the management, use, or operation of a Federal computer system within or under the supervision of the Federal agency. This includes contractors as well as employees of the agency. OMB Circular A-130, Appendix III, issued in 1996, enforces such mandatory training by requiring its completion prior to granting access to the system and through periodic refresher training for continued access. Therefore, each user should be versed in acceptable behavior — the rules of the system — before being allowed to use the system. Training should also inform the individual how to get help in the event of difficulty with using the system, and inform them of security incident and reporting procedures for the system.

Access provided to members of the public should be constrained by controls in the applications through which access is allowed, and training should be within the context of those controls and may consist only of notification at the time of access.

III.E.4.a. Security Awareness and Training Measures

All employees and contractors who are involved with the management, use, design, acquisition, maintenance, or operation of the support system should be aware of their security responsibilities and trained in how to fulfill them. Include information about the following in this section of the plan:

- The awareness program for the system (posters, booklets, trinkets).

- The type and frequency of system training provided to employees and contractor personnel (seminars, workshops, formal classroom, focus groups, role-based training, on-the-job).

- The nature of system security awareness provided during new employee orientation.

- The procedures for assuring that employees and contractor personnel have been provided adequate training.

Note: Contractor employees are required to receive the same level of automated information system security awareness and training as Federal employees. This training requirement should be included as appropriate in all contracts.

This page intentionally blank.

III.E.5. TECHNICAL CONTROLS

Technical controls are hardware and software controls used to provide protection from unauthorized access or misuse, to facilitate detection of security violations, and to support security requirements for associated applications.

Although the following controls are not addressed in detail in the OMB Circular A-130, Appendix III, issued in January, 1996, it states that “the technical security controls defined in OMB Bulletin No. 90-08 will continue.” To satisfy this requirement, and address the continuing importance of technical controls and their role in protection for every system, the following controls are incorporated from the preceding OMB Bulletin 90-08.

III.E.5.a. User Identification and Authentication

These are controls used to verify the identity of a station, originator, or individual prior to allowing access to the system, or specific categories of information within the system. Such controls may also be used to verify that only authorized persons are performing certain processing activities on the system. These controls include the use of passwords, tokens, or biometrics or other personal mechanisms to authenticate an identity.

User authentication is based on three categories of information: something the user knows, such as password; something the user possesses, such as a token; and some physical characteristic (biometrics) of the user, such as a fingerprint.

The most common type of authentication mechanism is the password. Password use became popular because passwords are easy to implement and provide a reasonable degree of authentication.

One of the weaknesses in using passwords to control access to systems and applications is the possibility of an individual user’s password being guessed. If users change their own passwords, they frequently select a password that is easy for them to remember (e.g., common word, name or date associated with a family member, sports-related word, or a repeat of their user identification [ID]). Software programs are available that are designed to be “password crackers.” These “password crackers” check passwords against dictionaries and other criteria for easy-to-guess passwords and provide reports that can be used to motivate users to change their passwords to something more secure.

WARNING: Many computer systems and software programs are shipped with administrative accounts that have preset default passwords. Because these passwords are standard, they are widely known. System Administrators frequently do not change these default passwords, creating a significant vulnerability for the system and any applications it supports.

Given the broader nature of system threats and increased use of IT to support mission-critical functions, more stringent authentication mechanisms (as stand alone controls or in combination with passwords) may be appropriate. Authentication methods employing a token or biometrics can provide a significantly higher level of security than passwords alone. Cryptography is often incorporated into advanced authentication systems, such as those using token or biometric methods.

Password systems, if structured properly, can provide several levels of controls, with assurances that only authorized users access the system or applications. Proper password structure meets the criteria from NIST FIPS 112, “Standard on Password Usage,” which is a mandatory standard for all Federal agencies.

In this section, describe the system’s access controls. The description should include consideration for the following items:

- Describe the method of user authentication (password, token, biometric).

- If a password system is used, provide the following specific information:

    - Allowable character set,
    - Password length (minimum, maximum),
    - Password aging time frames and enforcement approach,
    - Number of generations of expired passwords disallowed for use,
    - Procedures for password changes,
    - Procedures for handling lost passwords, and
    - Procedures for handling password compromise.
    - Procedures for training users and the materials covered.

Note: The recommended minimum number is six to eight characters in a combination of alpha, numeric, or special characters.

- Indicate the frequency of password changes, describe how password changes are enforced (e.g., by the software or System Administrator), and identify who changes the passwords (the user, the system, or the System Administrator).

- Describe any biometric controls used. Include a description of how the biometric controls are implemented on the system.

- Describe any token controls used on this system and how they are implemented.
    - Are special hardware readers required?
    - Are users required to use a unique Personal Identification Number (PIN)?
    - Who selects the PIN, the user or System Administrator?
    - Does the token use a password generator to create a one-time password?
    - Is a challenge-response protocol used to create a one-time password?

- Describe the level of enforcement of the access control mechanism (network, operating system, application).

- Describe how the access control mechanism supports individual accountability and audit trails (e.g., passwords are associated with a user identifier that is assigned to a single individual).

- Describe the self-protection techniques for the user authentication mechanism (e.g., passwords are stored with one-way encryption to prevent anyone [including the System Administrator] from reading the clear text passwords, passwords are automatically generated, passwords are checked against a dictionary of disallowed passwords, passwords are encrypted while in transmission).

- State the number of invalid access attempts that may occur for a given user identifier or access location (terminal or port) and describe the actions taken when that limit is exceeded.

- Describe the procedures for verifying that all system-provided administrative default passwords have been changed.

- Describe the procedures for limiting access scripts with embedded passwords (e.g., scripts with embedded passwords are prohibited, scripts with embedded passwords are only allowed for batch applications).

- Describe any policies that provide for bypassing of user authentication requirements, single-sign-on technologies (e.g., host-to-host, authentication servers, user-to-host identifier, group user identifiers) and any compensating controls.

III.E.5.b. Authorization/Access Controls

Describe hardware or software features that are designed to permit only authorized access to or within the application, to restrict users to authorized transactions and functions, and/or to detect unauthorized activities (e.g., access control lists).

Logical Access Controls

Computer system-based access control, or logical access control, is the mechanism used to specify "who" (subjects) can do "what" to resources controlled by the system or application (objects). Typical access modes are read, write, create, modify, execute programs, and delete data, programs and files. Access control safeguards also control the ability to access and use other system resources, such as external networks or communications, utility programs, or the computer operating system. Access control is discretionary when users can delegate access permissions to other users. This can be done directly by establishing access control lists or indirectly, by copying a file to a public area on the system. In this section, discuss the controls in place to authorize or restrict the activities of users and ADP personnel within the application.

- Describe formal policies that define the authority that will be granted to each user, or class of users. Indicate if these policies follow the concept of "least privilege" which requires identifying the user's job functions, determining the minimum set of privileges required to perform that function, and restricting the user to a domain with those privileges and nothing more.

- Identify whether the policies include "separation of duties" enforcement to prevent an individual from having all necessary authority or information access to allow fraudulent activity without collusion.

- Describe the application's capability to establish an Access Control List, or register of the users and the types of access they are permitted.

- Indicate whether a manual Access Control List is maintained.

- Indicate if the security software allows application owners to restrict the access rights of other application users, the general support system administrator, or operators to the application programs, data, or files.

- Describe how application users are restricted from accessing the operating system, other applications, or other system resources not needed in the performance of their duties.

- Describe any formal process requiring application owners to authorize all new users and define their individual rights or restrictions to read, write, create, modify, execute application programs, or delete application data or files.

- When the role or job function of a user changes, describe any formal process to review the access authorizations and change any rights or restrictions in line with the new requirements.

Note: It is particularly important that any rights no longer required for job performance be removed. Users will usually complain if restrictions prevent them from doing what they need to do, but rarely ask to have privileges taken away, even if they no longer need them.

- Indicate how often Access Control Lists are reviewed to identify and remove users who have left the organization or whose duties no longer require access to the application.

- Describe controls to detect unauthorized transaction attempts by authorized and/or unauthorized users.

- Describe policy or logical access controls that regulate how users may delegate access permissions or make copies of files or information accessible to other users. This "discretionary access control" may be appropriate for some applications, and inappropriate for others. Document any evaluation made to justify/support use of "discretionary access control."

- Indicate after what period of user inactivity the system automatically blanks associated display screens and/or after what period of user inactivity the system automatically disconnects inactive users or requires the user to enter a unique password before reconnecting to the system or application.

- Describe any restrictions to prevent users from accessing the system or applications outside of normal work hours or on weekends. Discuss in-place restrictions.

- Indicate if encryption is used to prevent unauthorized access to sensitive files as part of the system or application access control procedures. (If encryption is used primarily for confidentiality or integrity controls, include this information in the appropriate section.) If encryption is used as part of the access controls, provide information about the following:

  - What cryptographic methodology (e.g., secret key, public key) is used? If a specific off-the-shelf product is used provide the name of the product. If it meets Federal standards (e.g., Data Encryption Standard, Digital Signature Standard), include that information.

  - Discuss cryptographic key management procedures for key generation, distribution, storage, entry, use, destruction, and archiving.

Remote Users

Describe the type of remote access (dial, Internet) permitted and the functions that may be authorized for remote use (e-mail only, data retrieval only, full access). The following are some of the issues that should be addressed in this description:

Dial-In Access

- Document whether the system disconnects after a set number of improper password attempts, and describe any controls to prevent a person from re-dialing and trying additional passwords.

- Document who has access through the dial-in lines (by user type and number of users).

- Describe the procedures for obtaining the telephone numbers for dial-in lines, including controls to prevent unauthorized individuals from dialing in (e.g., the dial-in telephone numbers are unpublished and/or unlisted). If dial-in telephone numbers are published, describe why, where, and how extensively.

- Document whether the system/application has a dial-back capability.

Wide Area Networks

If your application is running on a system that is connected to the Internet or other wide area network(s), discuss what additional hardware or technical controls have been installed and implemented to provide protection against unauthorized system penetration and other known Internet threats and vulnerabilities.

- List the connections to the Internet or other wide area networks, including whether application users access the system through the Internet or a wide area network.

- Describe any type of secure gateway or firewall in use, including its configuration, (e.g., configured to restrict access to critical system resources and to disallow certain types of traffic to pass through to the system).

- Provide information regarding any port protection devices used to require specific access authorization to the communication ports, including the configuration of the port protection devices and if additional passwords or tokens are required.

- Identify whether internal security labels are used to control access to specific information types or files, and if such labels specify protective measures or indicate additional handling instructions.

- Indicate if host-based authentication is used. (This is an access control approach that grants access based on the identity of the host originating the request, instead of the individual user requesting access.)

Screen Warning Banners

Systems with external communications may need to alert potential users that inappropriate use may be subject to prosecution. Public Law 99-474 requires that a warning message be displayed, notifying unauthorized users that they have accessed a U.S. Government computer system and unauthorized use can be punished by fines or imprisonment. Although, the warning does not prevent unauthorized use of the system, it does facilitate prosecution of violators (i.e., failure to notify an unauthorized user that it is a Government system may make prosecution more difficult, regardless of how much damage is done to the system).

Some of the systems now in use are intended for unrestricted use by the general public (e.g., Internet-based systems used for widespread public information dissemination), a situation not prevalent when P.L. 99-474 was enacted. Thus, due to their adverse impact on the intended user population, highly restrictive warning banners may not be appropriate. The choice of which screen warning banner to implement is up to the system owner and should be based on system specific technology limitations, data sensitivity, or other unique system requirements. In this section describe the rationale for electing to use or not use warning banners and provide an example of the banners used. Where appropriate, state whether the warning banner was approved by the Department of Justice, Computer Crime Unit.

Don’t Forget

System opening banners/messages that include the word “Welcome” in the log-in sequence may be interpreted to authorize the use of the system by anyone. Such interpretations are not appropriate for systems restricted to access by pre-authorized Government users. If access to your system is limited to Government users (including contractors and other pre-authorized individuals) and your banner includes the word “Welcome” it should be removed to allow easier prosecution of unauthorized users.

Example Warning Banners

Banner	Selection Rationale	Approved by DOJ Computer Crime Unit
WARNINGWARNING**WARNING** This is a (Agency) computer system. (Agency) computer systems are provided for the processing of Official U.S. Government information only. All data contained on (Agency) computer systems is owned by the (Agency) *may be monitored, intercepted, recorded, read, copied, or captured in any manner and disclosed in any manner,* by authorized personnel. THERE IS NO RIGHT OF PRIVACY IN THIS SYSTEM. System personnel may give to law enforcement officials any potential evidence of crime found on (Agency) computer systems. *USE OF THIS SYSTEM BY ANY USER, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO THIS MONITORING, INTERCEPTION, RECORDING, READING, COPYING, OR CAPTURING and DISCLOSURE.* **WARNING**WARNING**WARNING**	System is for Government use only and all transmissions may be monitored.	Yes
WARNINGWARNING**WARNING** This is a United States (Agency) computer system, which may be accessed and used only for official Government business by authorized personnel. Unauthorized access or use of this computer system may subject violators to criminal, civil, and/or administrative action. All information on this computer system may be intercepted, recorded, read, copied, and disclosed by and to authorized personnel for official purposes, including criminal investigations. Access or use of this computer system by any person whether authorized or unauthorized, constitutes consent to these terms. **WARNING**WARNING**WARNING**	System is for Government use only. Monitoring is only performed in support of system operations and to investigate potential security events.	Yes
The seals, initials, and agency identification can not be used without the written permission of the agency.	Information dissemination system open to the general public. Associated risks are denial of access and transitory embarrassment to the agency.	No
None	Information dissemination system open to the general public. Associated risks are denial of access and transitory embarrasment to the agency.	No

III.E.5.c. Integrity Controls

Integrity controls are used to protect the operating system, applications, and information in the system from accidental or malicious alteration or destruction and to provide assurance to users that the information meets expectations about its quality and that it has not been altered.

Integrity is a quality of information that is based on attributes such as accuracy, timeliness, and completeness. System integrity is the quality of a system/software process that it does what it is supposed to do and nothing more.

Note: Operating system controls and system administration procedures, which are normally described in vendor supplied documentation, should be followed.

Discuss any controls in place to provide assurance to users that the information has not been altered and that the system functions as expected. Include any tests or evaluations that were used to determine compliance with security requirements during development or modification. Some of the controls that fit in this category include:

Malicious Programs

In this section, provide a brief overview and reference the items in the discussion of configuration management and personnel controls that describe control measures intended to prevent installation of software that performs unauthorized functions.

Virus Protection

One of the most significant controls for smaller systems, including file servers, is virus detection and elimination software. It may also be appropriate to install this type of software on secure gateways, depending on the threat. Virus detection/ elimination software could cause a slow down of data transfer. In this section describe the virus detection/elimination approach used for the system. Include in this discussion the following items:

- A list of components on which virus detection software is installed (client, server, firewall) and a rationale for its use. Also include a statement as to whether the license is current.

- Procedures for updating virus signature files.

- Procedures for automatic and/or manual virus scans (automatic scan on network log-in, automatic scan on client/server power on, automatic scan on diskette insertion, automatic scan on download from an unprotected source such as the Internet, scan for macro viruses).

- Virus eradication and reporting procedures.

- Virus eradication support availability (e.g., central technical support specialists, incident response capability).

Message Authentication

Message authentication is a method using cryptographic approaches to ensure that the sender of a message is known and that the message has not been altered during transmission. State whether message authentication has been determined to be appropriate for your system. If message authentication is used, describe the methodology.

Integrity Verification

Integrity verification programs can be used by applications to look for evidence of data tampering, errors, and omissions. Techniques include consistency and reasonableness checks and validation during data entry and processing. These techniques can check data elements, as input or as processed, against expected values or ranges of values. Message authentication techniques may also be used to ensure data integrity while in transit or storage.

Describe the integrity controls used within this system.

Reconciliation

Reconciliation routines use checksums, “hash totals,” record counts, and other approaches to detect unauthorized changes to data and/or program files. These approaches generate a mathematical value based on the contents of a particular file which is stored external to the file. To verify the integrity of the file, the mathematical value is recomputed on the current file and compared with the previously generated value. The two values should match.

Describe any reconciliation routines used by the system. Include a description of the actions taken to resolve any discrepancies.

Digital Signature

Digital signatures provide an extremely high level of integrity assurance. Federal agencies using digital signatures must use technology that conforms with FIPS 186, “Digital Signature Standard” and FIPS 180, “Secure Hash Standard” issued by NIST, unless a waiver has been granted. Digital signatures provide assurance of the identity of the originator, that the originator cannot falsely deny having signed the file (non repudiation), that the file has not been modified after being signed, and that the originator intends to be bound by the contents of the file. Digital signatures are designed to meet the standards of proof required by law. Digital signatures are required to replace a hand-written signature on a commitment document (e.g., contract, funds transfer document) or if the results of a risk analysis shows that level of protection is necessary and cost-effective.

Electronic signatures that meet some, but not all of the digital signature standard may also be used to provide lower levels of integrity control. For most systems, these less secure “electronic signatures” may be adequate integrity protection.

In this section describe any use of digital or electronic signatures. Address the following specific issues:

- State the digital signature standards used. If the standards used are not NIST standards, please state the date the waiver was granted and the name and title of the official granting the waiver.

- Describe the use of electronic signatures and the security control provided.

- Discuss cryptographic key management procedures for key generation, distribution, storage, entry, use, destruction and archiving.

III.E.5.d. Audit Trail Mechanisms

Audit trail mechanisms are controls that provide a system monitoring and recording capability to retain a chronological record of system activities. Audit trails enable reconstruction of a transaction from its inception to final results—including any modification of files. One type of audit trail, keystroke monitoring, is usually used to protect systems from intruders who access the system without authority or in excess of their assigned authority. Section III.E.5.b. contains information about screen warning banners required on systems with keystroke monitoring capability.

Other audit trails are event-oriented and include system, application, and user audit capability. System audit trails are generally used to monitor and fine-tune system performance. They should be able to record all log-on attempts, user identification, date/time, devices used, functions performed, applications accessed and user log-off, but may not be able to log events within applications. Application audit trails may be used to detect flaws in applications, or violations of security policy committed with an application. User audit records are generally used to hold individuals accountable for their actions. An audit trail should include sufficient information to establish what events occurred, when they occured, and who caused them (i.e., the associated user identifier).

No matter how much information is captured by the audit trail, it serves no purpose unless it is routinely monitored for unusual activity (e.g., violations of policy or rules of behavior or unauthorized access attempts). Reviews include:

- Regularly scheduled analysis of audit trail reports by system and application owners or automated information system security personnel.

- Special reviews after the occurrence of an unanticipated event.

- Real-time audit analysis by automated audit tools with manual follow-up of identified anomalies.

Access to on-line logs or audit reports must be strictly controlled to prevent destruction or modification of the records. Audit trail records may be used as legal evidence and protecting their integrity is critical. In addition, audit trails may record information about individual user activities which must be protected for confidentiality. Audit trail records should be protected by strong access controls to help prevent unauthorized access. The use of encryption and digital signatures may also be considered for audit logs of very sensitive applications.

In this section, describe the measures used to protect system usage and audit trail logs. Include consideration for the following items in this discussion:

- List the system usage and audit trail logs (including the events logged and data elements recorded) produced by the general support system.

- Describe any linkages between logs maintained by the system and the supported applications.

- Describe how the actions of individual users of the system may be monitored through the system logs.

- Describe procedures used for reviewing logs and audit trail reports.

III.E.5.e. Confidentiality Controls

Confidentiality controls provide protection for information that must be held in confidence and protected from unauthorized disclosure. The controls may provide information protection at the user site, at a computer facility, and/or while in transit.

Confidentiality can be protected by physical security barriers to buildings, rooms, equipment, or while transporting media or printed material. It can also be protected by logical barriers in the hardware/software, such as authentication and logical access controls and monitoring audit logs and reports. Procedures such as personnel screening and granting access based on need-to-know are very effective. One of the most significant and cost-effective controls is providing adequate security awareness and training to employees and users about the importance of maintaining confidentiality of information against unauthorized disclosure. Encryption provides the strongest and most secure protection against loss of data/system confidentiality.

Discuss any controls used to protect the confidentiality of information from unauthorized disclosure. If the information is already covered in other sections of the plan (e.g., operational controls or technical controls), do not repeat it here. Include references to the section numbers where it is contained.

III.E.5.f. Incident Response Capability

Security incidents, whether caused by viruses, hackers, or software bugs, are becoming more common. When faced with a security incident, an agency should be able to respond in a manner that both protects its own information and helps to protect the information of others who might be affected by the incident. To address this concern, agencies should establish formal incident response mechanisms. It should be noted that incident response includes a set of complex responsibilities requiring individuals to have extensive technical training and experience in various hardware and telecommunications and is usually handled at the agency level. Awareness and training for individuals with access to the system should include how to use the system’s incident response capability.

To be fully effective, incident handling must also include sharing information concerning common vulnerabilities and threats with those in other systems and other agencies. OMB Circular A-130, Appendix III, issued in 1996, directs agencies to implement such sharing arrangements and tasks NIST to coordinate those agency activities Government-wide. It also directs the Department of Justice to provide appropriate guidance on pursuing legal remedies in the case of serious incidents.

Describe the incident handling procedures for the system. Include consideration for the following items in this discussion:

- Formal incident response capability (in-house or external) and reporting;

- Procedures for obtaining the services of the incident response capability (e-mail address, telephone number, point of contact);

- Incident notification/alert procedures;

- Response to alerts received (e.g., implementation of vendor-provided security “patches”);

- Sources for receipt of security alerts;

- Penetration testing; and

- Analysis of system logs and audit trails for suspect activity.

III.E.6. CONTROLS OVER THE SECURITY OF APPLICATIONS

The security of each application that processes on a general support system may affect the security of other applications sharing the general support system. One of the roles of general support system security is to ensure separation of applications such that the potential for one application to adversely affect another is minimized. To accomplish this objective, the manager of the general support system should understand the risk that each application represents to the system. If not, plans for greater understanding of that risk should be described (e.g., application users that have access to programming capability represent a higher risk to the support system than those that are confined to individual application functions—similarly, applications that utilize dial-up communications represent a higher risk).

It is the responsibility of the application owner to provide information to the general support system regarding the security requirements of their application. The general support system has no responsibility to provide security beyond their own system protection levels unless specifically requested by the application owners.

In this section, describe the controls used to maintain separation between applications. This discussion should include the following items:

- Controls used to restrict application access to the network and/or computer operating system.

- Procedures for authorizing and reviewing system access authority.

- Protection mechanisms for systems with dial access or wide area network access (e.g., Internet access).

- List the name, unique identifier, and owner of supported applications. Also describe any unique support requirements.

This page intentionally blank.

IV. ADDITIONAL COMMENTS

This section provides an opportunity to include additional comments about the security of the subject system and any perceived need for guidance or standards. Use this section to discuss any features or administrative standards that are in place within your environment that may not be covered in the rest of the plan. Also, include information in this section about planned major changes that might affect this system in the future (e.g., the mainframe hardware for this system will be replaced and upgraded by new super computer hardware during the third quarter of FY98; this local area network is being expanded to provide service to two additional organizations on three more floors of Building ABC; or this system will be relocated when the organization moves to Silver Spring, MD in October, 1999).

Include discussion of any Federal or organizational security policies, standards or guidelines that apply.

This page intentionally blank.

APPENDIX A — GLOSSARY

Acceptable Risk is a risk that is acceptable to responsible management, due to the cost and magnitude of implementing countermeasures.

Accreditation is the authorization and approval, granted to a major application or general support system to process in an operational environment. It is made on the basis of a certification by designated technical personnel that the system meets pre-specified technical requirements for achieving adequate system security. See also ***Authorize Processing, Certification*** and ***Designated Approving Authority.***

Acquisition/Development/Installation/Implementation Controls refers to the process of assuring that adequate controls are considered, evaluated, selected, designed and built into the system during its early planning and development stages and that an on-going process is established to ensure continued operation at an acceptable level of risk during the installation, implementation and operation stages.

Authorize Processing management authorization should be based on an assessment of management, operational and technical controls. By authorizing processing in a system the Designated Approving Authority (DAA) accepts the risk associated with it. See also ***Accreditation, Certification,*** and ***Designated Approving Authority.***

Availability Protection requires backup of system and information, contingency plans, disaster recovery plans, and redundancy. Examples of systems and information requiring availability protection are time share systems, mission-critical applications, time and attendance, financial, procurement, or life-critical.

Awareness, Training and Education includes (1) awareness programs set the stage for training by changing organizational attitudes toward realization that the importance of security and the adverse consequences of its failure; (2) the purpose of training is to teach people the skills that will enable them to perform their jobs more effectively; (3) education is more in-depth than training and is targeted for security professionals and those whose jobs require expertise in automated information security.

Certification is the technical evaluation that establishes the extent to which a computer system, application or network design and implementation meets a pre-specified set of security requirements. See also ***Authorize Processing*** and ***Accreditation.***

Confidentiality Protection requires access controls such as user ID/password, terminal identifiers, restrictions on actions like read, write, delete, etc.. Examples of Confidentiality protected information are personnel, financial, proprietary, trade secrets, internal agency, investigations, other Federal agency, national resources, national security, and high or new technology under Executive Order or Act of Congress.

Designated Approving Authority (DAA) is the senior management official who has the authority to authorize processing (accredit) an automated information general support system or major application and accept the risk associated with the system.

Development Controls see ***Acquisition/Development/Installation/Implementation Controls.***

General Support System is an interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, facilities, and people and provides support for a variety of users and/or applications. Individual applications support different mission-related functions. Users may be from the same or different organizations.

Individual Accountability requires individual users to be held accountable for their actions after being notified of the rules of behavior in the use of the system and the penalties associated with the violation of those rules.

Installation/Implementation Controls see
Acquisition/Development/Installation/Implementation Controls.

Integrity Protection requires validation controls and security embedded during system design and development. Examples of integrity protected information are financial, proprietary, trade secrets, investigations, mission critical, operational, national resources, and high or new technology under Executive Order or Act of Congress.

Major Application is an application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. A breach in a major application might comprise many individual application programs and hardware, software, and telecommunications components. Major applications can be either a major software application or a combination of hardware/software where the only purpose of the system is to support a specific mission-related function.

Networks include communication capability that allows one user or system to connect to another user or system and can be part of a system or a separate system. Examples of networks include local area network or wide area networks, including public networks such as the Internet.

Operational Controls are the day-to-day procedures and mechanisms used to protect operational systems and applications. Operational controls affect the system and application environment.

Risk is the possibility of harm or loss to any software, information, hardware, administrative, physical, communications, or personnel resource within an automated information system or activity.

Risk Management is the on-going process of assessing the risk to automated information resources and information, as part of a risk-based approach used to determine adequate security for a system by analyzing the threats and vulnerabilities and selecting appropriate cost-effective controls to achieve and maintain and acceptable level of risk.

Rules include the set of rules of behavior that have been established and implemented concerning use of, security in, and acceptable level or risk for the system. Rules will clearly delineate responsibilities and expected behavior of all individuals with access to the system. Rules should cover such matters as work at home, dial-in access, connection to the Internet, use of copyrighted works, unofficial use of Federal Government equipment, the assignment and limitation of system privileges, and individual accountability.

Sensitive Information refers to information that requires protection due to the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information. The term includes information whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary information, records about individuals requiring protection under the Privacy Act, and information not releasable under the Freedom of Information Act.

Sensitivity in an information technology environment consists of the system, data, and applications which must be examined individually and in total. All systems and applications require some level of protection for confidentiality, integrity, and availability which is determined by an evaluation of the sensitivity and criticality of the information processed, the relationship of the system to the organization's mission and the economic value of the system components.

System is a generic term used for briefness to mean either a major application or a general support system.

A ***System*** is identified by logical boundaries drawn around the various processing communications, storage, and related resources. They must be under same direct management control (not responsibility), perform essentially the same function, reside in the same environment, and have the same characteristics and security needs. A system does not have to be physically connected.

System Operational Status is either (a) Operational - system is currently in operation, (b) Under Development - system is currently under design, development, or implementation, or (c) Undergoing a Major Modification - system is currently undergoing a major conversion or transition.

Technical Controls consist of hardware and software controls used to provide automated protection to the system or applications. Technical controls operate within the technical system and applications.

Threat is an activity, deliberate or unintentional, with the potential for causing harm to an automated information system or activity.

Vulnerability is a flaw or weakness that may allow harm to occur to an automated information system or activity.

APPENDIX B — REFERENCES

Federal Laws and Regulations

Privacy Act of 1974, Public Law 93-579

Computer Fraud & Abuse Act of 1986, as amended, Public Law 99-474

Computer Security Act of 1987, Public Law 100-235

Paperwork Reduction Act of 1978, as amended in 1995, U.S. Code 44 Chapter 35

Freedom of Information Act of 1974, 5 U.S. Code Section 552

OMB Circular A-123, Internal Control Systems

OMB Circular A-127, Financial Management Systems

OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources

OMB Bulletin 90-08, Guidance for Preparation of Security Plans for Federal Computer Systems That Contain Sensitive Information

Federal Information Processing Standards

FIPS Publication 31, Guidelines for ADP Physical Security and Risk Management

FIPS Publication 41, Computer Security Guidelines for Implementing the Privacy Act of 1974

FIPS Publication 46-1, Data Encryption Standard

FIPS Publication 48, Guidelines on Evaluation of Techniques for Automated Personal Identification

FIPS Publication 73, Guidelines for Security of Computer Applications

FIPS Publication 74, Guidelines for Implementing and Using the NIST Data Encryption Standard

FIPS Publication 81, DES Modes of Operation

FIPS Publication 83, Guideline on User Authentication Techniques for Computer Network Access Control

FIPS Publication 87, Guidelines for ADP Contingency Planning

FIPS Publication 88, Guideline on Integrity Assurance and Control in Database Administration

FIPS Publication 94, Guideline on Electrical Power for ADP Installations

FIPS Publication 102, Guideline for Computer Security Certification and Accreditation

FIPS Publication 112, Standard on Password Usage

FIPS Publication 113, Standard on Computer Data Authentication

FIPS Publication 139, Interoperability and Security Requirements for Use of the Data Encryption Standard in the Physical Layer of Data Communications

FIPS Publication 140-1, Security Requirements for Cryptographic Modules

FIPS Publication 141, Interoperability and Security Requirements for Use of the Data Encryption Standard with CCITT Group 3 Facsimile Equipment

FIPS Publication 171, Key Management Using ANSI X9.17

FIPS Publication 180-1, Secure Hash Standard

FIPS Publication 181, Automated Password Generator

FIPS Publication 185, Escrowed Encryption Standard

FIPS Publication 186, Digital Signature Standard

FIPS Publication 188, Standard Security Label for Information Transfer

FIPS Publication 190, Guideline for the Use of Advanced Authentication Technology Alternatives

FIPS Publication 191, Guideline for the Analysis of Local Area Network Security

<u>Selected NIST Special Publications</u>

SP 500-120, Security of Personal Computer Systems

SP 500-133, Technology Assessment: Methods for Measuring the Level of Computer Security

SP 500-134, Guide on Selecting ADP Backup Process Alternatives

SP 500-156, Message Authentication Code (MAC) Validation System: Requirements and Procedures

SP 500-157, Smart Card Technology: New Methods for Computer Access Control

SP 500-166, Computer Viruses and Related Threats: A Management Guide

SP 500-172, Computer Security Training Guidelines

SP 500-173, Guide to Auditing for Controls and Security: A System Development Life Cycle Approach

SP 800-2, Public-Key Cryptography

SP 800-3, Establishing a Computer Security Incident Response Capability

SP 800-4, Computer Security Considerations in Federal Procurements: A Guide for Procurement Initiators, Contracting Officers, and Computer Security Officials

SP 800-5, A Guide to the Selection of Anti-Virus Tools and Techniques

SP 800-6, Automated Tools for Testing Computer System Vulnerability

SP 800-7, Security In Open Systems

SP 800-9, Good Security Practices for Electronic Commerce, Including Electronic Data Interchange

SP 800-10, Keeping Your Site Comfortably Secure: An Introducement to Internet Firewalls

SP 800-12, An Introduction to Computer Security: The NIST Handbook

SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems

NISTIR 4749, Sample Statements of Work for Federal Computer Security services: For Use In-House or Contracting Out

NISTIR 4939, Threat Assessment of Malicious Code and External Attacks

This page intentionally blank.

APPENDIX C — SECURITY PLAN OUTLINE MAJOR APPLICATIONS

I. SYSTEM IDENTIFICATION

I.A. Responsible Organization
I.B. System Name/Title
I.C. System Category
I.D. System Operational Status
I.E. General Description/Purpose
I.F. System Environment and Special Considerations
I.G. System Interconnection/Information Sharing
I.H. Information Contact(s)

II. SENSITIVITY OF INFORMATION HANDLED

II.A. Applicable Laws or Regulations Affecting the System
II.B. General Description of Sensitivity

III. SYSTEM SECURITY MEASURES

III.A. Risk Assessment and Management
III.B. Review of Security Controls
III.C. Applicable Guidance
III.D. Rules
III.E. Security Control Measures

III.E.1. MANAGEMENT CONTROLS

III.E.1.a. Assignment of Security Responsibility
III.E.1.b. Personnel Security

III.E.2. DEVELOPMENT/IMPLEMENTATION CONTROLS

III.E.2.a. Authorize Processing
III.E.2.b. Security Specifications
III.E.2.c. Design Review and Testing

III.E.3. OPERATIONAL CONTROLS

III.E.3.a. Physical and Environmental Protection
III.E.3.b. Production, Input/Output Controls
III.E.3.c. Contingency Planning
III.E.3.d. Audit and Variance Detection
III.E.3.e. Application Software Maintenance Controls
III.E.3.f. Documentation

III.E.4. SECURITY AWARENESS AND TRAINING

III.E.4.a. Security Awareness and Training Measures

III.E.5. TECHNICAL CONTROLS

III.E.5.a. User Identification and Authentication
III.E.5.b. Authorization/Access Controls
III.E.5.c. Public Access Controls
III.E.5.d. Data Integrity/Validation Controls
III.E.5.e. Audit Trail Mechanisms

III.E.6. COMPLIMENTARY CONTROLS PROVIDED BY SUPPORT SYSTEM

IV. ADDITIONAL COMMENTS

APPENDIX D — SECURITY PLAN OUTLINE GENERAL SUPPORT SYSTEMS

I. SYSTEM IDENTIFICATION

I.A. Responsible Organization
I.B. System Name/Title
I.C. System Category
I.D. System Operational Status
I.E. General Description/Purpose
I.F. System Environment and Special Considerations
I.G. System Interconnection/Information Sharing
I.H. Information Contact(s)

II. SENSITIVITY OF INFORMATION HANDLED

II.A. Applicable Laws or Regulations Affecting the System
II.B. General Description of Sensitivity

III. SYSTEM SECURITY MEASURES

III.A. Risk Assessment and Management
III.B. Review of Security Controls
III.C. Applicable Guidance
III.D. Rules
III.E. Security Control Measures

III.E.1. MANAGEMENT CONTROLS

III.E.1.a. Assignment of Security Responsibility
III.E.1.b. Personnel Controls

III.E.2. ACQUISITION/DEVELOPMENT/IMPLEMENTATION CONTROLS

III.E.2.a. Authorize Processing
III.E.2.b. Acquisition Specifications

III.E.3. OPERATIONAL CONTROLS

III.E.3.a. Physical and Environmental Protection
III.E.3.b. Production, Input/Output Controls
III.E.3.c. Contingency Planning
III.E.3.d. Audit and Variance Detection
III.E.3.e. Hardware & System Software Maintenance Controls
III.E.3.f. Documentation

III.E.4. SECURITY AWARENESS AND TRAINING

III.E.4.a. Security Awareness and Training Measures

III.E.5. TECHNICAL CONTROLS

III.E.5.a. User Identification and Authentication
III.E.5.b. Authorization/Access Controls
III.E.5.c. Integrity Controls
III.E.5.d. Audit Trail Mechanisms
III.E.5.e. Confidentiality Controls
III.E.5.f. Incident Response Capability

III.E.6. CONTROLS OVER THE SECURITY OF APPLICATIONS

IV. ADDITIONAL COMMENTS

INDEX

Page